CODE OF CONDUCT FOR PROCESSING OF PERSONAL DATA BY LAWYERS

under the EU General Data Protection Regulation (GDPR)

Slovenská advokátska komora

Approved by the Office for Personal Data Protection of the Slovak Republic
by Decision No 00676/2018-Os-9 of 4 December 2018
and entered into force on 10 December 2018.

Preamble

(1) Processing of personal data that relate to clients and third parties by lawyers is an inevitable part of practice of the members of the legal profession, fulfilment of legal and regulatory obligations by lawyers and protection of legitimate interests of both clients and lawyers.

(2) Legal profession helps enforce the fundamental right to fair trial which belongs to natural and legal persons while it stems from the nature of such right that its enforcement may, to necessary extent, contravene with the right to data protection of persons against or for which such right to fair trial is enforced.

(3) Lawyers are governed by specific legal provisions, in particular by the Act on Legal Profession and by profession rules adopted by the Slovak Bar Association, that justify the specific approach that lawyers should take to protection of personal data under the GDPR.

(4) The protection of personal data by lawyers is essential for maintaining the duty of confidentiality by lawyers. Violation of the protection of personal data may compromise the duty of confidentiality. As the one who guarantees confidentiality, trust, expertise and ethics, the lawyer should lead the way in personal data protection.

(5) The relationship between the rights of data subjects under the GDPR and lawyer's duty to maintain confidentiality and protect the client's interests must be brought into harmony and balance. The rights that data subjects have under the GDPR are not absolute, and any exceptions to them should be adapted to obligations that lawyers have under existing legislation in the strict sense and to their status and roles they have in society in the broader sense.

(6) The aim of this Code is to promote the relationship of trust between lawyers and their clients while increasing the transparency of lawyers in the processing of personal data about clients and other individuals.

(7) In accordance with Article 24 (3) of the GDPR, compliance with the Code may be used as an element to demonstrate the compliance with obligations that lawyers have under the GDPR. As set in Article 83 (2) of the GDPR, in any decisions on whether to impose an administrative fine by the Office for Personal Data Protection and on the amount of the administrative fine in each individual case a due regard should be given to specific circumstances, including adherence to approved codes of conduct.

NOW, THEREFORE, IN VIEW OF THE ABOVE, THE SLOVAK BAR ASSOCIATION DECIDED TO ADPOPT THIS CODE AS FOLLOWS:

1 Introductory provisions

1.1 Scope of the Code

1.1.1 This Code applies to all lawyers registered in the list of lawyers maintained by the Slovak Bar Association. For the purposes of this Code, a 'lawyer' under the preceding sentence is any person (including a legal person) authorised under the Act on the Legal profession to provide legal services in the Slovak Republic, provided that such person has an establishment in the Slovak Republic and that the processing of personal data occurs in the context of activities carried out in this establishment, whether or not the processing of personal data takes place within the Slovak Republic or not.[1]

1.1.2 This Code does not apply to such processing of personal data by a lawyer that is not covered by the GDPR and Act on Personal Data Protection.

1.2 Legal nature of the Code

This Code is intended to contribute to a correct application of the GDPR, taking into account the specifics of the legal profession sector and the specific needs of small firms and lawyers that are micro, small and medium-sized enterprises. At the same time, this Code should help simplify the interpretation of the GDPR for the legal professionn sector.

1.3 Relationship between this Code and competences of the Office for Personal Data Protection

1.3.1 This Code is without prejudice to the competences of the Office for Personal Data Protection under the GDPR or Act on Personal Data Protection in relation to lawyers as controlled entities or parties to proceedings.

1.3.2 Although compliance with this Code may be used as an element to demonstrate compliance with the GDPR, this Code does not exempt lawyers from their obligation to ensure compliance with the GDPR or other privacy laws. Every lawyer is required to comply with the GDPR and other privacy laws as their own responsibility and in accordance with this Code.

1.3.3 This Code is without prejudice to any options that data subjects have to bring any claims to the Office for Personal Data Protection, Slovak Bar Association or competent court.

1.4 Relationship with other legislation

1.4.1 The GDPR is the European Union's general data protection law and also applies to the processing of personal data by lawyers, if its scope is applicable. The other legislation that is applicable to legal profession complements, specifies or restricts the GDPR as a general regulation.

1.4.2 In the context of processing of personal data for purposes stated in this Code, the GDPR shall be the general regulation while:

i. provisions of Section 2, Section 5, second and third part of Act on Personal Data Protection are not applicable to lawyers;
ii. provisions of Section 1, Section 3, Section 4, fourth, fifth and sixth part of Act on Personal Data Protection are applicable to lawyers.

1.5 Explanation of core concepts

1.5.1 Personal data

Personal data means any information relating to an identified or identifiable natural person (data subject). When determining whether any specific information qualifies as personal data, lawyers should not base their conclusions on the fact that any personal data need not, in itself, have the ability to identify a natural person. For any information to qualify as personal data, it is sufficient if such information can be attributed to a natural person that is identified or identifiable.

Example: An email, phone number or IP address need not, as such, enable identification of a natural person. However, if this information relates to a particular identified natural person (e.g. a person recognised by

[1] This Code should apply to such persons whenever under the GDPR the Slovak law applies to the processing of personal data performed by such persons.

the lawyer) or an identifiable natural person, then it qualifies as personal data. Types of personal data are not limited to the name, surname, birth number, place of residence, etc. Under its definition, personal data may be any information. The important thing is not the type of information but that it can be attributed to a particular natural person.

1.5.2 Identified natural person

According to the Office for Personal Data Protection: "*A natural person can be in general considered to be identified if he or she is distinguishable within a group of persons from all other members of such group, so that their identity is clearly identified*."[2]

Example: For a lawyer, an identified natural person may be their client or employee. Information relating to these persons is personal data (even if they are sole traders). Information that relate to legal entities (persons) is not personal data.

1.5.3 Identifiable natural person

An identifiable natural person is a person who can be identified by means reasonably likely to be used, such as singling out, by the controller or another person to identify the natural person directly or indirectly. Theoretically, every natural person is identifiable. To assess whether a natural person is identifiable in view of personal data definition (i.e. whether information qualifies as personal data), the test of reasonable likelihood as set out in Recital 26 of the GDPR is decisive.

Example: For a lawyer, an identifiable natural person may be an unknown offender whose identity the lawyer should help to uncover in the interests of his client in the criminal proceedings (such as a person captured in a camera recording). Information relating to an identifiable person (e.g. a camera recording) is then personal data.

1.5.4 Test of reasonable likelihood

To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. Test of reasonable likelihood is not met when the identification of data subject is prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.[3] As a result of the application of test of reasonable likelihood it may also be concluded in a specific case that the processed information is not personal data because there is no reasonable likelihood of using means to identify the natural person to whom such information relates.

Example: It may stem from criminal proceedings that the offender cannot be identified. Information that relate to a person that cannot be identified should not be considered as personal data.[4]

1.5.5 Filing system

Under the GDPR, the term of filing system has little to do with an IT system, software, database or application. As per Article 4 (6) of the GDPR, a filing system means *"any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis."* This term is used in the GDPR solely in relation to the material scope of the GDPR set out in Article 2 (1) to determine whether personal data processed by other than automated means falls within the scope of the GDPR. In other words, under the GDPR the term of filing system is a test to assess whether personal data processed manually (i.e. in paper or physical form) should fall under the GDPR or not.

Example: Doorplates or room plates in a lawyer's office that contain, for example, lawyer's name, surname and title do not constitute a filing system and, even if such information falls under the definition of personal data, the GDPR does not apply to their processing in such form. A client file[5] in which the lawyer processes

[2] Methodological guidance of the Office for Personal Data Protection no. 1/2013 on the concept of personal data, 1.7.2013, p. 2.
[3] Judgment of the Court of Justice of the European Union in case C 582/14 (Breyer v. Germany) of 19 October 2016, para 46.
[4] In these cases, the lawyer cannot tell beforehand whether or not the offender will be identified. However, by taking on a criminal case and providing legal advice, the lawyer increases the likelihood that the offender will be identified for the benefit of the client. The recommended practice is therefore to treat such information as personal data in similar situations, and this Code helps the lawyer to ensure that additional obligations relating to the processing of personal data affect their obligations that they have in the exercise of advocacy as little possible.
[5] Resolution of the Council of the Slovak Bar Association No. 29/11/2011 of 1 December 2011 on the recommended way of keeping client files.

personal data of the client or counterparty in paper form may qualify as a filing system[6] and therefore the GDPR may apply to such processing. If paper documents containing personal data are scanned and sent by email or stored in a computer, electronically processed personal data are generated to which the filing system "exception" is not applicable. However, the GDPR application to paper documents or files does not affect the legal and professional obligations of a lawyer in relation to documents and information concerned.

1.5.6 Data subject

Data subject is an identified or identifiable natural person to whom personal data relates.

Example: From the perspective of a lawyer, typical data subjects are a client, counterparty or employee (natural person). In relation to employees or bodies of legal persons, the lawyer should proceed accordingly in line with Section 2.6 below.

2 Status of lawyers and other parties in processing of personal data

2.1 Lawyer as a controller

2.1.1 A controller is a person who alone decides about purposes ("why") and means ("how") of processing of personal data or a person whose status of a controller stems from Union or Member State law which provides for purposes and means of processing for those persons.

Example: A typical controller is an employer in relation to an employee, a service provider or seller of goods in relation to a customer or a public authority in relation to citizens.

2.1.2 In the exercise of legal profession, and for other purposes for the processing of personal data provided in this Code, lawyers typically act as controllers. The right of lawyers to process the personal data of clients and other natural persons during the practice of their lawyer profession explicitly arises from the provisions of Section 18 (6) of the Act on Legal Profession:

"A lawyer shall process personal data of clients and other individuals to the extent necessary for pursuing legal profession in compliance with separate legal rules *(Note: GDPR)*. When processing data according to the first sentence of this paragraph a lawyer is considered to be a data controller pursuant special legal regulation *(Note: Article 4 (7) of the GDPR)."*

2.1.3 A lawyer shall not be considered as a controller if the lawyer obtains personal data randomly without prior identification of the purposes and means of processing. In this case, the GDPR does not apply to the processing of such personal data. The preceding sentence does not apply if the lawyer subsequently determines the purpose and means of processing after the lawyer has randomly obtained personal data.

Example: This case may reflect situations where personal data is provided to a lawyer in error, by mistake, by speculation, or as personal data that has not been requested and the lawyer is not interested in further processing of such personal data for any purpose, for instance when the lawyer mistakenly receive an email containing personal data. Keeping this data, for example for its return to the authorised person or its deletion within a reasonable time, does not constitute the processing of personal data falling within the scope of the GDPR. However, if the lawyer started to use or used the personal data so collected, he or she would be regarded as a controller in relation to the purposes of processing and the GDPR would apply.

2.2 Lawyer as a processor

A processor is a person who processes personal data on behalf of a controller under such controller's instructions. The processor, unlike the controller, is not authorised to decide on the purposes and means of processing and is therefore not authorised to formally take decisions regarding the processing of personal data. Although the lawyer acts on behalf of the client and within the limits of the law and under the client's instructions, this does not apply to the lawyer's entitlement to process personal data that relates to clients and other natural persons in such lawyer's own name under Section 18 (6) of the Act on the Legal profession, nor in view of lawyer's independent status during the practice of legal profession and the duty to use their knowledge and experience, arguments based on facts and law and options given by law for the benefit of their client. However, this does not mean that the lawyer cannot process personal data as a processor, e.g. for other processing purposes.

[6] On term "filing system", please refer to decision of CJEU in C 25/17.

2.3 Lawyers as joint controllers

2.3.1 Joint controllers are two or more controllers that jointly determine the purpose and means of processing.

Example: Joint controllers may be, as an example, several lawyers pursuing legal profession in a partnership under Section 13 of the Act on the Legal Profession or, where appropriate, several lawyers associating for a purpose other than the joint practice of legal profession under Section 48 of the Rules of Professional Conduct for Lawyers.

2.3.2 Joint controllers are obliged to make a mutual arrangement taking into account the requirements set out in Article 26 (1) and (2) of the GDPR. As per Article 26 (2) second sentence, the essence of such arrangement between the joint controllers should be published.

Example: The essence of an arrangement may be published by lawyers that are joint controllers for example on their website as part of their Privacy Policy (Annex 2 of this Code).

2.4 Substituting lawyer

2.4.1 Substitution is lawyer's statutory authorisation (Section 16 of the Act on the Legal Profession), for which the lawyer does not need the prior consent of the client, but such substitution must not be against the will of the client. Under Section 20 of the Rules of Professional Conduct for Lawyers, the substituting lawyer is to the authorising lawyer in a similar position as the lawyer has towards the client, and the authorising lawyer continues to communicate with their clients under Section 6 of the Rules of Professional Conduct for Lawyers as the client's lawyer.

2.4.2 Relationship between the substituting lawyer and the authorising lawyer may qualify as the relationship pursuant to Article 29 of the GDPR where the authorising lawyer acts as the controller and the substituting lawyer acts as the person acting under the authority of the controller.[7] The substituting lawyer is the person that has access to personal data and may process personal data only on controller's instructions with an exception of situation where processing activities are required under EU or Member State law.

2.4.3 In the case of substitution, lawyers may also agree to proceed as described in Section 2.3 above as joint controllers. In such case, they are obliged to define in their arrangement how the GDPR obligations are divided among them, in particular in relation to their clients. If the lawyers do not make the joint controllers arrangement, Article 29 of the GDPR is applicable and the authorising lawyer is responsible for handling requests of data subjects. The substituting lawyer is required to grant to the authorising lawyer any reasonable assistance in dealing with requests of data subjects in relation to such substitution.

2.5 Group of law firms

2.5.1 Groups of law firms should transparently define the position of individual companies or persons belonging to the same group in the form of internal policies, memorandum or agreements.

2.5.2 A group of law firms may constitute joint controllers under Article 26 of the GDPR. Sharing, making available, providing and processing of personal data that relate to clients or employees within the same group of law firms may represent a legitimate interest of the group; and in such case consent of data subjects is not required for such sharing or joint processing.[8] This is without prejudice to any obligations concerning confidentiality.

2.5.3 The group of law firms may include entities that play a role in the provision of legal services by providing support to the group and that may have access to personal data processed by the group. Law firms should ensure that the entities mentioned above are included in the arrangements under point 2.5.1 above and that these entities are bound to maintain confidentiality to the same extent as law firms.

2.6 Employees of the lawyer

2.6.1 Employees and other professional staff of the lawyer under Section 65 of the Act on Legal Profession are considered, in the processing of personal data, as persons acting under the authority of the lawyer and processing of their personal data in accordance with law, regulations and professional regulations is considered as processing of personal data by the lawyer.

---

[7] "acting under the authority" as in English version of the GDPR.

[8] GDPR explicitly states in Recital 48: *"Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing* ***of clients' or employees'*** *personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected."*

2.6.2 Under Section 79 (2) of the Act on Personal Data Protection, the lawyer as a controller is obliged to impose confidentiality on all natural persons come into contact, at such lawyer, with personal data and this duty of confidentiality must survive the termination of employment of these persons. The duty of employees and other professional staff involved in the provision of legal services to maintain confidentiality follows directly from Section 23 (8) of the Act on Legal Profession. Nevertheless, the practice recommended by lawyers is to incorporate such employee's duty to maintain confidentiality in their policies.

2.7 Clients

2.7.1 The processing of personal data about clients that are natural persons is the processing of personal data by the lawyer, regardless of whether the legal representation concerns the client's private, work or business matter. In the provision of legal services, clients as natural persons are data subjects to the lawyer.

2.7.2 Clients that are legal persons are not data subjects. Only natural persons may be data subjects. However, during the provision of legal services or in connection with other purposes, the lawyer processes personal data relating to natural persons who act as executive representatives, employees or members of other bodies of legal persons.

2.7.3 Pursuant to Recital 14, the GDPR should not apply to personal data contained in the name of a legal entity nor to contact details of legal persons.[9] The interpretation of the provision in question is not yet clear in practice. However, in the provision of legal services this interpretative problem is removed by the Act on the Legal profession that entitles lawyers to process personal data about clients *and other natural persons*.

2.8 Other natural persons

Other natural persons within the meaning of Section 18 (6) of the Act on Legal Profession are natural persons other than lawyer's clients. The lawyer is authorised to process personal data about such other natural persons for the purposes of practice of law to the extent necessary. In the provision of legal services, the other natural persons are data subjects to a lawyer. A lawyer typically does not collect personal data directly from the other natural persons but from the client, public sources or public authorities. The Code uses the term 'other natural persons' in this meaning.

Example: The counterparty or its employees, the contractual party of the client, the spouse, the children or other family members of the client, other parties as a client, etc.

3 Purposes and legal grounds for processing

3.1 Introduction

3.1.1 The purpose of personal data processing explains *why personal data is processed*. The purpose of the processing is determined by the controller or the controller has such purpose under law. It is typical for regulated professions that processing purposes follow from legislation, even though such legislation may allow some contractual freedom in concluding relationships that are regulated.

3.1.2 Multiple purposes of processing that concern lawyers directly follow from legislation that mandates or permits lawyers to process certain personal data about their clients and other natural persons. Although in some cases the legislation does not explicitly describe the specific purpose of the processing, this is not absolutely required for determining the lawyer as a controller. It is sufficient that the law requires the lawyer to fulfil a certain obligation or to allow them to act in a certain way.

3.1.3 It is of the essence to differ between purposes and legal grounds of processing. Legal ground *explains on what legal entitlement the processing of personal data takes place*. The legal ground is, among other things, relevant for determining whether the specific processing of personal data is legal.

3.1.4 Each purpose may have several legal grounds, but always at least one.[10] If the purpose has a number of possible legal grounds, the lawyer is entitled to rely on any one of them and to adapt its compliance with all related obligations under the GDPR to such legal ground.

---

[9] The GDPR explicitly states in Recital 14: *"This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person."*

[10] Article 29 Data Protection Working Party Opinion 15/2011 on the definition of consent, p. 8: *"In some transactions a number of legal grounds could apply, at the same time. In other words, any data processing must at all times be in conformity with one or more legal grounds. This does not exclude the simultaneous use of several grounds, provided they are used in the right context."*

3.1.5 The purposes of processing provided in this Code are a selection of the most commonly used (typical) purposes of processing operations by lawyers. Lawyers are required to consistently analyse the actual purposes of processing they conduct in ensuring compliance with the GDPR.

3.2 Typical purposes of processing

The processing of personal data by the lawyer may typically involve the processing of personal data for the following purposes:

Purposes of processing	Primary legal ground	Related legislation
Practice of profession (provision of legal services)	Compliance with legal obligation pursuant to Article 6 (1) (c) GDPR, performance of contract pursuant to Article 6 (1) (b) GDPR, legitimate interest pursuant to Article 6 (1) (f) GDPR	Act on Legal profession, Rules of Professional Conduct for Lawyers, Civil Code and Commercial Code
Provision of non-legal services	Compliance with legal obligation pursuant to Article 6 (1) (c) GDPR, performance of contract pursuant to Article 6 (1) (b) GDPR, legitimate interest pursuant to Article 6 (1) (f) GDPR	Public Sector Partners Act, Act on e-Government, Civil Code, Commercial Code, Act on Lease of Non-Residential Premises
Compliance with laws and regulations of Slovak Bar Association	Compliance with legal obligation pursuant to Article 6 (1) (c) GDPR, legitimate interest of lawyers pursuant to Article 6 (1) (f) GDPR or public interest pursuant Article 6(1) (e) GDPR.	GDPR, Act on Legal profession, Rules of Professional Conduct for lawyers, Anti-Money Laundering Act, Act on Whistleblowing, GDPR
Purposes concerning protection of legitimate interests	Legitimate interest of lawyers or third parties pursuant to Article 6 (1) (f) GDPR.	GDPR, Civil Code, Commercial Code, Criminal Code, Criminal Procedure, Civil Procedure, Code of Civil Non-Contentious Procedure, Code of Administrative Judicial Procedure, Code Administrative Procedure, Act on Offences
Marketing purposes	Consent of data subject pursuant to Article 6 (1) (a) GDPR or legitimate interest of lawyers or third parties pursuant to Article 6 (1) (f) GDPR.	Act on Legal profession, Act on Electronic Communications, Act on Advertising, Consumer Protection Act, Civil Code
Statistical purposes, archiving purposes in public interest and purposes of historical and scientific research	The legal ground that allowed collection of personal data for original purposes (compatible purposes) in the light of Article 89 GDPR.	Act on Archives
Personnel & Payroll	Compliance with legal obligation pursuant to Article 6 (1) (c) GDPR, performance of contract pursuant to Article 6 (1) (b) GDPR, alternatively legitimate interest pursuant to Article 6 (1) (f) GDPR	Labour Code, Act on Legal profession and other legislation
Accounting & Tax purposes	Compliance with legal obligation pursuant to Article 6 (1) (c) GDPR	Specific law in the area of accountancy and taxes

3.3 Further explanation of typical purposes of processing

3.3.1 The above purposes of processing give a general overview of the different types of lawyer's purposes of processing as are typically defined by lawyers. In practice, each purpose may have several modalities, legal grounds, and may involve various processing operations. In addition, some purposes may require clarification or division into multiple separate processing purposes in a particular situation.

Example: Marketing purposes are listed as a separate purpose for greater clarity but it is, in practice, advisable to distinguish at least sending newsletters as a separate purpose. Similarly, the purposes that relate to legitimate interests should in practice be more clearly defined and distinction should be made between legitimate interests as various purposes of processing. Therefore, the typical purposes given above are not necessarily a full list of lawyer's purposes and should only serve as a guidance for lawyers who should also take into consideration the following Sections as they define individual purposes.

3.3.2 Practice of profession (provision legal services) may involve the processing of personal data that is necessary, for example, for the following lawyer activities:

- Preparing the offer of legal services at client's request, including participation in client's selection procedures;
- Assessing the client in terms of a potential conflict of interest;
- Forming a contractual relationship with a client including pre-contractual relationships;
- Verifying the client's identity;
- Representing clients before court, public authorities and other legal entities;
- Defence in criminal proceedings;
- Providing legal advice;
- Drafting documents on legal acts;
- Drafting of legal analyses;
- Management of clients' property;
- Other forms of legal advice and legal assistance;
- Communicating with clients and other natural persons that concerns the practice of profession or a contractual relationship with a client;
- Search for evidence in favour of the client;
- Legal advice as a Data Protection Officer pursuant to the GDPR;
- Finding the identity of clients using witnesses, statements provided by municipality, or documentary evidence.

3.3.3 The provision of non-legal services may involve the processing of personal data that is necessary, for example, for the following lawyer activities:

- Performance of function of an authorised person under the Public Sector Partners Act;
- Authorisation of contracts, including search for information about persons that might suffer damage as a result of conclusion of a contract;
- Carrying out conversion and guaranteed conversion;
- Rental of real estate, flats and non-residential premises providing exclusively basic services that ensure normal operation of real estate, flats and non-residential premises.

3.3.4 Compliance with laws and regulations of the Slovak Bar Association may include the processing of personal data that is necessary, for example, for the following lawyer's activities:

- Compliance with obligations set by anti-money laundering legislation;
- Internal administrative activities related to or supporting the provision of legal and non-legal services;
- Keeping records of time, actions and advice given to the client;
- Administration and control of the contract between the client and the lawyer;
- Keeping the lawyer's files;
- Whistleblowing.

3.3.5 The protection of legitimate interests during the practice of legal profession mainly concerns the security of law firm's premises, facilities and software. A legitimate interest may serve also as an additional legal ground for the processing of personal data for purposes which the law foresees but where it insufficiently specifies the conditions for processing of personal data. A typical example of when the processing of personal data may be made on the legal ground of protecting legitimate interests and, at the same time, on other legal grounds, is security of personal data. Lawyers are required to take reasonable safeguards for the protection of personal data under the GDPR, where the adoption of security measures may be not only a way to protect legitimate interests but also may be an obligation under a generally binding legal regulation that is the GDPR. The choice of the legal ground for the processing of data in similar cases should be left to the lawyer as the controller that determines the purposes and means of processing as well which legal grounds for their processing of personal data they choose.

3.3.6 In terms of security, the protection of lawyer's legitimate interests of lawyers may be translated into:

- Physical protection of law firm's premises using CCTV systems or security guard;
- Recording and control of access to electronic systems, applications and websites (logging in);
- Using cryptographic tools.

3.3.7 Marketing activities may involve the processing of personal data that is necessary, for example, for the following lawyer activities:

- Sending newsletters, legal news, invitations to special lectures and seminars, festive greetings;
- Marketing and customer satisfaction surveys;
- Disclosure of information about legal advice given, including client references;
- Provision of personal data during participation in ratings, rankings or lists of recommended law firms.

3.3.8 Lawyers collect personal data that is processed for purposes shown above mainly through communication with clients, written correspondence, by telephone or by electronic means. In practice, there may be situations where the lawyer's client provides to the lawyer personal data about other natural persons that the lawyer must or may process for their own purposes. Lawyers do not obtain consent from natural persons as their entitlement to process personal data in the practice of their profession results directly from the Act on Legal profession.

3.3.9 Lawyers are entitled to require from clients, potential clients or persons that claim to be their clients their identity documents for identity verification purposes or for fulfilment of their legal or contractual obligations and are authorised to scan, copy or otherwise record such documents.

3.4 Cookies

3.4.1 Information obtained by interaction of visitor's web browser and website and/or the use of cookies (such as IP address, operating system, time of website visit, geographic location, content displayed, previous content history, etc.) may be processed by lawyers using various analytical tools on their website. This is with the purpose of storing or gaining access to information stored in the end-device of the user, which is, pursuant to Section 55 (5) of Act on Electronic Communications generally[11] conditioned by obtaining a consent from website users on the basis of clear and complete information about the purpose of their processing, while respective web browser settings (such as 'do not block cookies') is also considered as consent. The lawyer should check whether similar tools or technologies are used in connection with their website and follow the recommendations given below.

Example: There are many free online solutions to check if your website is using cookies. One can also learn more about cookies through browser Google Chrome. By right-clicking over the website (or pressing CTR + U), you can search for "cookies settings" page code. E.g. "cookieSettings": {"isRestrictiveCookiePolicyEnabled": false} means that the site does not accept the use of cookies.

3.4.2 If the lawyer uses cookies that in itself does not mean that processing of personal data takes place.

Example: If a lawyer's website collects only basic anonymous data about the number of visits, time and geographical location without reasonable likelihood of using lawyer's or third-party's means party to identify the natural person (i.e. without the practical possibility of attributing this information to specific individuals), this does not amount to processing of personal data. This is without prejudice to the provisions of Section 55 (5) of the Act on Electronic Communications.

3.4.3 In all cases of using cookies, the lawyer is required to inform visitors about the use and purposes of cookies, for example using the Privacy Policy template given in Annex 2.

3.4.4 It is a recommended practice for lawyers to limit the scope of information processed through cookies. This is especially true in relation to IP addresses and so-called advertising IDs[12] that to highest degree increase the likelihood that processing of personal data takes place. If the lawyer considers that the use of cookies on his or her website amounts to processing of personal data, the lawyer must comply with additional obligations under the GDPR.

[11] In light of Section 55 (5) of Act on Electronic Communications: *"This shall not prevent any* ***technical storage of data or access thereof for the sole purpose of the conveyance or facilitation of the conveyance of a communication by means of a network*** *or if it* ***unconditionally necessary for the provider of an information society service to provide information society services*** *if explicitly requested by the user."*

[12] These are, in particular, the identifiers that are used to identify Google and Facebook users. While the lawyer may not be able to associate a given identifier with a particular person, it is sufficient, from the perspective of the definition of personal data, if there is a reasonable likelihood of using third party identification means (Google and Facebook). Based on information collected, for example, from a lawyer's website, these companies can then display to visitors similar content on their own or on other platforms because they know that a particular user browsed, at a specified location and in a specified time, sites with the content of legal advice.

4 Principles relating to processing of personal data

4.1 Introduction

The purpose of this part of the Code is to explain in detail seven basic principles of processing of personal data under Article 5 of the GDPR in legal profession. These basic principles are a source of almost all additional obligations that lawyers as controllers have on the one hand and all rights that data subjects have on the other. However, these additional obligations and rights have their limits and there are legitimate exceptions that cannot be interpreted as violation of basic principles of processing resulting from them.

4.2 Lawfulness, fairness and transparency

4.2.1 Personal data must be processed by lawyers lawfully, fairly and in a transparent manner in relation to the data subject. Processing of personal data is lawful when the lawyer processes personal data under at least one of the legal grounds for processing specified in the GDPR. Consent with the processing of personal data is just one of the legal grounds and is not a universal legal ground. By its nature a consent may be withdrawn by the data subject at any time, which would make it impossible to achieve some of the processing purposes. In practice, lawyers usually rely on legal grounds arising from special regulations, performance of the contract, and the protection of legitimate interests where consent to the processing of personal data is not necessary. As explained below, in some cases lawyers rely on more than one legal ground at the same time to achieve the intended purpose of processing.

Example: In the provision of legal services, the lawyer does not rely on the consent with the processing of personal data of their clients or other natural persons. The lawyer processes personal data of these persons without their consent within the purpose of practice of profession (provision of legal services) as this purpose of processing follows from Section 18 (6) of the Act on Legal profession. At the same time, however, it can be argued that the processing of personal data for the purpose of practice of profession (provision of legal services) can be considered necessary in order to perform a contract with the data subject. In such cases, the lawyer is free to choose a more appropriate legal ground (at least one). This Code supports the choice of a scheme which the lawyer uses to comply with their legal obligations because the scheme also involves other natural persons with whom the lawyer has no a contract; however, nothing prevents the lawyer from relying on other legal grounds, such as performance of the contract or legitimate interest pursuant to Article 6 (1) (b) and (f) GDPR, respectively.

4.2.2 Where the lawyer relies on a legal ground that is based on specific legislation, it is not necessary for the specific legislation to determine the precise conditions for the processing of personal data. On the contrary; in practice, it is common that specific legislation explicitly mentions none or only some of the particularities of processing of personal data. This is also presumed by the GDPR, as in Article 6 (1) (c) it conditions the use of legal ground to comply with specific legislation by stating that the processing is necessary for compliance with a legal obligation. The GDPR continues in Article 6 (3) by provisioning that the purpose of processing shall in such case be determined either by Union or Member State law to which the controller is subject. It is therefore not necessary for the specific law to explicitly define or characterise the purpose. It is sufficient if the regulation clearly establishes an obligation to be fulfilled by controller or an authorization to process personal data for a specific purpose foreseen by the law. The exact wording of the purpose should be drafted by the controller who bears the burden of proof that the purpose so determined is based on the given law.

4.2.3 The term "law of the Member State" includes not only acts (laws) but also any generally binding legislation. The term "legal obligation" should be understood as any legal obligation and may therefore also be an obligation arising from binding professional regulations of the Slovak Bar Association.

4.2.4 If the lawyer relies on a legal ground based on a specific law, the purpose of such lawyer's processing may also constitute a legitimate interest of the lawyer or another person under Article 6 (1) (f) of the GDPR. If the lawyer is able to demonstrate compliance with the terms of using the legal ground of legitimate interest, the lawyer can thereby prove the lawfulness of the processing of personal data to a greater extent than is necessary ulfilfor the compliance with a legal obligation under such law.

4.2.5 Lawyers may also rely on the legal ground of "performance of the contract", governed by Article 6 (1) (b) of the GDPR. For the use of this legal ground, the form or nature of the contract with the data subject is not relevant and, at the same time, that legal ground permits the processing of personal data under the so-called pre-contractual relationships with data subject.

4.2.6 It is specific to the performance of legal profession that the fulfilment of contractual relations is at the same time

subject to regulation under special legislation. In a situation where the processing of personal data is necessary for the performance of the contract and is at the same time necessary to perform legal obligation of a lawyer, lawyers are entitled to rely on any of these legal grounds and accordingly adapt the ulfilmentcompliance with other obligations under the GDPR.

4.2.7 Lawyers may, for the purposes of processing of personal data, rely on the legal ground of consent of data subject to process their personal data for some purposes. Lawyers do so by default in cases where it is not possible to rely on any other legal ground or if consent is explicitly required by law. Consent may be given in any way, whether written, electronic, audio or audiovisual, but always subject to the terms of Article 7 of the GDPR. When assessing whether a consent is freely given, utmost account shall be taken of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

4.2.8 The principle of fair and transparent processing requires the data subject to be informed of the existence of the processing operation and its purposes. Lawyers comply with the principle of fair and transparent processing by providing information to their clients and to the public, through privacy policies available at the website, in other contractual documentation, in communication with clients, and at the same time through this Code. Although most of this information is open to the public, the principle of fair and transparent processing is not absolute. During the provision of legal services by lawyers this principle is limited to persons to whom the lawyer owes the obligation to maintain confidentiality under Section 23 of the Act on Legal profession.

4.2.9 The general principle of fair and transparent processing is closely related to the adaptation of lawyer's information obligations while obtaining personal data in Articles 13 and 14 of the GDPR as well as upon request by data subject under Article 15 of the GDPR. The same applies to the general obligations laid down in Article 12 of the GDPR. These provisions result in a number of exceptions which the Code sets out in relation to lawyer in further Sections.

4.3 Purpose limitation

4.3.1 Principle of purpose limitation requires that personal data be collected for specified, explicit and legitimate purposes and forbids processing in a manner that is incompatible with those purposes.

Example: This Code encourages lawyers to notify data subjects about all purposes of processing at the same time, for example through privacy policies published on their websites (see Annex 2 below).

4.3.2 In Article 6 (4), the GDPR provisions so-called compatibility test of the new purpose of processing with the original purpose of the processing based on which personal data was obtained. If the lawyer obtains personal data from the outset with an intention to process personal data for various purposes in line with principle of lawfulness, fairness and transparency (existence of legal ground for processing), these purposes do not fall within a compatibility test. The compatibility test results in usability of the original legal ground for processing by the lawyer for a new purpose of processing, as explained in Recital 50 of the GDPR: *"In such a case, no legal basis separate from that which allowed the collection of the personal data is required."* Some purposes are automatically compatible with the original purpose, such as purposes of archivation in the public interest (Act on Archives), scientific or historical research purposes and statistical purposes set out in Article 89 of the GDPR. With these purposes there is no need to conduct a compatibility test pursuant to Article 6 (4) of the GDPR. However, Article 89 of the GDPR does not represent a legal ground for processing of personal data for these purposes.

Example: The lawyer collects personal data of clients for the purpose of practice of profession (providing legal services). If the lawyer later decides to process these personal data for statistical purposes or for purposes of archiving in the public interest, the lawyer shall consider these other purposes as being automatically compatible with the original purpose without obtaining specific legal bases in relation to those other purposes, provided guarantees referred to in Article 89 of the GDPR are met.

4.4 Data minimisation

4.4.1 Principle of data minimisation requires lawyers to process personal data that are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Excessive processing of personal data i.e. processing more personal data than needed for achieving the purpose is considered to be a breach of the pertinent principle. The lawyer is responsible for demonstrating the need of all processed personal data for achieving the purposes of processing.

4.4.2 However, the principle of data minimisation does not mean that each lawyer processes the same personal data. The necessary extent of the processed personal data is always considered according to circumstances

of the specific case of providing legal advice. The lawyer is obliged, inter alia, to protect and enforce the rights and interests of the client, to use consistently all legal remedies and to apply, in the best interests of the client, everything he or she considers to be beneficial, taking into account the usefulness and economy of the legal services provided. The data minimisation principle shall not limit the lawyer's professional judgment to what is or may be in the interest of the client. The processing of personal data to the extent necessary to protect the interests of the client according to the lawyer is the processing of personal data in accordance with the pertinent principle.

4.4.3 Principle of data minimisation is complemented by requirements of data protection by default according to Article 25 (2) of the GDPR.

4.5 Accuracy

4.5.1 Principle of accuracy requires lawyers to process personal data in an accurate way and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. However, the principle of accuracy does not refer to the absolute objective accuracy of the processed personal data but to the accuracy of the personal data for the purposes for which the personal data are processed. Some purposes may, for example, require explicitly to proceed with the processing of objectively incorrect personal data. The accuracy of processed personal data is assessed in terms of processing purposes.

Example: The lawyer maintains email communication between the client and another person who has attempted to mislead the client by misrepresentation. The person then asks the controller to correct incorrect personal data about the person. The lawyer is not obliged to correct the personal data because the personal data are not incorrect for the purpose of processing (practice of profession) and subsequent court proceedings - they serve as evidence against the person kept in the client's interest in the original (objectively incorrect) wording. If, on the other hand, the client asks for a correction of his or her permanent residence due to its change, the lawyer is obliged to correct these incorrect personal data about the client because from the point of accounting and tax the personal data are incorrect.

4.5.2 The principle of accuracy therefore constitutes an obligation that requires reasonable efforts by the controller to ensure the accuracy of the processed personal data and the other party does not exempt from the responsibility to provide correct personal data.

Example: It complies with the principle of accuracy if a contract between a lawyer and a client includes the obligation for the client to report changes to their personal data to a lawyer.

4.5.3 It is specific to practice of legal profession that the lawyer must not verify the truthfulness or completeness of factual information provided by clients (that may include personal data of individuals) without the consent of the client. If the lawyer has reasonable doubts about their veracity or completeness, the client shall be instructed about the possible legal consequences of the information so obtained.

Example: It complies with the principle of accuracy acording to the GDPR if a client knowingly or unknowingly provides the lawyer with improper personal information and the lawyer in accordance with pertinent obligation processes personal data for the purpose of pursuing the profession e.g. in criminal proceedings in the interest of the client.

4.6 Storage limitation

4.6.1 Principle of storage limitation requires lawyers to keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Given that personal data are at the same time processed by lawyers for multiple purposes, it is not a breach of this principle if one of the purposes of processing ends, but the lawyer does not delete the personal data because they are required for different purpose. These other purposes may be defined from the moment when the personal data are collected or later during the processing in accordance with the purpose specification principle that allows processing for other purposes through a test of compatibility of the new purpose with the original purposes.

4.6.2 Lawyers should adopt internal rules setting retention periods of personal data for individual purposes. The storage limitation principle serves as an aid to setting the limit or upper limit of retention periods. However, the retention periods are set by the controller, since only the controller can assess the need for the identification of data subjects for the purposes of the processing of personal data. In some cases, retention periods may stem from

specific regulations. However, some specific rules only provide for a minimum statutory retention period (e.g. the obligation to retain personal data for at least 5 years), with potential longer retention periods in respective cases.

4.6.3 The purpose of archivation in the public interest under Article 89 of the GDPR is closely related to the Act on Archives whereas the public interest pursued by this law is the preservation of archival documents that have permanent documentary value for the history of Slovakia and the Slovaks. The processing of personal data for the purpose of archiving in the public interest may include, in addition to maintenance of archives, the administration of active records of originators of records which originators can be also lawyers. However, there is nothing to prevent the lawyer from complying with the obligations under the Act on Archives on the basis of the legal ground for fulfilling legal obligations outside the regime of Article 89 of the GDPR. The Act on Archives imposes an obligation on the lawyer as an originator of records to record incoming and generated active records during the retention period, which represents the period during which lawyers need active records for their activity. The lawyer may set the appropriate time limits of their own and are eligible to follow the recommendations and practice of the Ministry of the Interior of the Slovak Republic. Retention periods under the Act on Archives are not general periods of retention of personal data under the GDPR, as retention periods under the Act on Archives refer only to archiving in the public interest and/or to performance of obligations under the Act on Archives and do not apply to other purposes. Where the GDPR Article 89 regime applies, retention periods only start to pass after the retention periods under original processing purposes have expired. Active records may or may not contain personal details of data subjects, including copies of the contractual documentation. According to the GDPR, reasonable safeguards for the rights and freedoms of the data subject shall be in place during archiving in the public interest. These safeguards ensure the implementation of technical and organizational measures, in particular to ensure compliance with the principle of data minimisation. Adopted records retention policy and / or schedule under the Act on Archives is / are technical and organizational measures that monitor compliance with the principle of data minimisation. Lawyers should restrict access to documents retained under the Act on Archives in their similar internal policies. If the lawyer proceeds under the Act on Archives, he or she is obliged to erase personal data only in the discarding procedure under this Act and this procedure is in accordance with the principle of storage limitation.

4.6.4 The principle of storage limitation is complemented by requirements of data protection by default under Article 25 (2) of the GDPR.

4.7 Integrity and confidentiality

The principle of integrity and confidentiality requires lawyers to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The principle is complemented by further requirements related to security of personal data in Section 2 Chapter IV of the GDPR, specifically in Articles 32 to 34, as explained in Section 8 of this Code below.

4.8 Accountability

4.8.1 Pursuant to principle of accountability, lawyers are responsible for, and must be able to demonstrate, compliance with basic principles of processing as set out in Article 5 (1) of the GDPR. The GDPR does not set forth specific ways of demonstration of compliance with basic principles of processing and compliance with this obligation is thus left to the discretion of the controller.

Example: Compliance with principle of accountability may be demonstrated by lawyers by adherence to basic principles of processing, e.g.:

- ***by adopting privacy policies pursuant to Article 24 (2) of the GDPR reflecting aspects of data protection by design and default according to Article 25 of the GDPR;***
- ***by concluding contracts with processor or joint controllers pursuant to Articles 26 or 28 of the GDPR;***
- ***by maintaining records of processing activities pursuant to Article 30 of the GDPR;***
- ***by cooperating with the Office for Personal Data Protection of the Slovak Republic during exercise of its tasks and competences pursuant to Article 31 of the GDPR;***
- ***by adopting appropriate security measures pursuant to Articles 32,33 and 34 of the GDPR;***
- ***by evaluating measures taken to ensure the security of processing and assessing their efficiency;***
- ***by conducting data protection impact assessment and potential prior consultation pursuant to Article 35 and 36 of the GDPR;***
- ***by regular training of staff in data protection;***
- ***by designating data protection officer pursuant to Articles 37 to 39 of the GDPR;***

- ***by complying with rules and appropriate safeguards during cross-border transfers of data to third countries or international organisations;***
- ***by adhering to approved certification mechanisms, seals and marks pursuant to Article 42 et seq. of the GDPR;***
- ***by adhering to this Code;***
- ***by designating "authorised persons", in particular in view of limiting their number if possible;***
- ***by designating contact persons serving as a contact point for data subjects and handling their requests;***
- ***by publishing the contact details of data protection officer if applicable; or***
- ***by any other means.***

4.8.2 This Code provides recommendations related to adoption of minimum internal documentation of lawyers in Section 12 below.

5 Processing of special categories of personal data

5.1 General conditions

5.1.1 In practice, special categories of personal data are processed for the same purposes along with common personal data. If the lawyer relies on any exception to the prohibition under Article 9 (2) of the GDPR in relation to special categories of personal data, the attroney must at the same time proceed on the legal ground resulting from Article 6 of the GDPR. Exceptions to this rule may be made only where the conditions laid down in Article 9 (2) already contain the conditions required by the legal basis under Article 6 (1) of the GDPR, such as explicit consent under Art. 9 (2) (a) of the GDPR that already contains the requirements for consent under Art. 6 (1) a) of the GDPR.

5.1.2 Unlike in the previous legislation under Directive 95/46/EC, as implemented by Act no. 122/2013 Coll. on the Protection of Personal Data, birth numbers and personal data relating to criminal convictions and offences are not considered as special categories of personal data. These personal data may be processed on the legal bases referred to in Article 6 of the GDPR. This is without prejudice to additional obligations arising in connection with the processing of personal data set out, for example, in Article 10 of the GDPR and Section 78 (4) the Act on Personal Data Protection.

5.1.3 From the historical perspective, a photograph of data subject was also considered a special category of personal data. The GDPR changes this approach because under Recital 51 the processing of photographs should not systematically be considered as the processing of special categories of personal data as these would be captured under the definition of biometric data only when processed through specific technical means allowing the unique identification or authentication of a natural person. To illustrate this point, a normal security camera recording or a copy of an identity document, including photos on that document, do not meet this condition.

5.2 Cases of processing of special categories of personal data

5.2.1 Lawyers may also process special categories of personal data when giving legal advice. These include the data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or concerning a natural person's sex life or sexual orientation.

5.2.2 The processing of special categories of personal data is allowed if it is necessary for the establishment, exercise or defence of legal claims under Article 9 (2) (f) of the GDPR. One can imagine, in the practice of legal profession, cases where the processing of such data may occur e.g. in case of providing legal advice on discriminatory disputes, disputes relating to the protection of fundamental human rights and freedoms, crimes of extremism or advice in claiming damages caused by the exercise of medical profession. It is also necessary to process sensitive personal data to the extent necessary for the purpose of exercising of legal profession.

5.2.3 The processing of special categories of personal data may be necessary for reasons of substantial public interest, on the basis of Union or Member State law that is proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; under Article 9 (2) (g) of the GDPR. Such an important public interest may arise, for example, from specific legislation aiming to prevent criminal activities or other activities such as Anti-Money Laundering Act, Criminal Code or Act on Corporate Criminal Liability.

5.2.4 The processing of special categories of personal data may also be carried out on the basis of the consent of data subject in accordance with Article 9 (2) (a) of the GDPR. The difference of this consent from the "normal"

consent under Article 6 (1) (a) of the GDPR is its expression. The condition of expression refers to the way the consent is given by data subject.[13] Explicit consent is the opposite of implicit consent and is therefore an agreement expressing an explicit legal act (e.g. by signing or ticking a box) while it is sufficiently clear from the wording or manner of expressing the consent that the consent relates to special categories of personal data.

6 Rights of data subjects

6.1 Handling of requests made by data subjects

6.1.1 When informing, communicating or responding to requests made by data subjects, the lawyer must proceed in compliance with Article 12 of the GDPR. The lawyer should facilitate the exercise of data subject rights by providing various alternatives for lodging their requests.

Example: The data subject that claims their rights pursuant to the GDPR may be, in principle, any natural person. Only after the content of data subject's claim has been considered, the lawyer should proceed to a possible refusal of the request, which refusal must also be justified.

6.1.2 If the lawyer has reasonable doubts as to the identity of the natural person making the request, the lawyer may request additional information to confirm such natural person's identity.

Example: If the client as data subject makes a GDPR request from an email address different from the one the client usually uses, the lawyer should verify if it is in fact the client, for example, by confirming such client's request by phone. The method of verifying the client's identity should always be appropriate in relation to the data subject. Under no circumstances may the lawyer provide information about the client to an unverified third party.

6.1.3 The general time limit for handling the request of data subject under Articles 15 to 22 of the GDPR is one month after the receipt of the request. The lawyer is entitled to decide to extend this one month period by up to two more months, taking into account the complexity of the request and the total number of requests received at that time by the lawyer. Whenever the lawyer decides to extend the time limit, the lawyer is required to inform the data subject of any such extension together with the reasons why the lawyer missed the original one month period.

6.1.4 If the lawyer does not take action on the request of the data subject, the lawyer is obliged to inform the data subject of the reasons for not taking the actions and on the possibility of lodging a complaint with the Office for Personal Data Protection of the Slovak Republic or seeking a judicial remedy within one month of receipt of the request. This also includes situations where the lawyer did not take action, for example because the data subject did not provide additional information within a time period of one month to verify his or her identity or did not make his or her general request more specific. After provision of additional information by the data subject, a new one month period starts to run.

6.1.5 If requests of the data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the lawyer is entitled to refuse to act on the request or charge a reasonable fee, taking into account the lawyer's administrative costs, as decided by the lawyer. The lawyer is required to assess in each individual case whether the data subject's request is manifestly unfounded or excessive and must be able to prove it. As a recommended general rule, if there is a repeated request from the same data subject,the lawyer should, after a specific assessment of the situation, consider such request as excessive only where there is less than 6 months between the same requests.

Example: Manifestly unfounded requests by data subjects are, in particular, requests:

- ***on the basis of which a data subject other than the client or client's representative asks for access to information in respect of which the lawyer is required to maintain confidentiality;***
- ***that are by nature explicitly vexatious against the lawyer's employees or the lawyer himself;***
- ***that are vulgar or contain elements of racial, ethnic, gender, sexual or religious hatred;***
- ***that are so general or so incomprehensible that the lawyer cannot objectively identify from the request what right the data subject seeks;***
- ***by which the data subject requests information, notifications or measures that do not explicitly follow from Articles 15 to 20 of the GDPR;***
- ***that repeatedly address the same issue that has been already explained by the lawyer to the data subject, where it must be clear to the data subject from the circumstances of the case that there was no reason***

[13] Article 29 Working Party Guidelines on consent under Regulation 2016/679 dopted on 28 November 2017 as last revised and adopted on 10 April 2018, p. 18.

why the lawyer's response should be changed;

- ***where the data subject makes video, audio or audiovisual recordings of lawyer´s employees or lawyers;***
- ***where the data subject acts aggressively, under the influence of alcohol or narcotics or threatens the safety of other persons occupying the same space.***

6.1.6 When handling the requests of the data subject, the lawyer proceeds adequately according to the internal privacy policy, if adopted.

6.1.7 Handling certain requests from data subjects by refusal by the lawyer is also foreseen in Section 18 (8) of the Act on Legal profession for the purpose of maintaining the lawyer's confidentiality:

***"*A lawyer is not obliged to provide information on the personal data processing, facilitate access or enable data portability pursuant special legal regulation (*footnote: Article 14 (5) (d) 15 (4) and Article 20 (4) of the GDPR)* if it may lead to breach of professional duty of secrecy in compliance with this Act."**

6.2 Information provided to data subjects

6.2.1 The lawyer is entitled to comply with the information obligations under Articles 13 and 14 of the GDPR in any way, irrespective of the form of information provided. The significant difference between the obligations is that the lawyer proceeds pursuant to Article 13 of the GDPR only if personal data are obtained directly from data subjects. Lawyers proceed pursuant to Article 14 of the GDPR only if personal data are not obtained directly from data subjects while Article 14 of the GDPR provides several exceptions to the rule.

Example: The lawyers typically proceed under Article 13 of the GDPR in relation to their clients or employees. The lawyers typically proceed under Article 14 of the GDPR in relation to natural persons who are employees of their corporate client or in relation to a counterparty and other natural persons about whom the lawyer is processing personal data during the exercise of his profession (e.g. witness, other party to proceedings, invited party, intervener, the other party to a contract, etc.).

6.2.2 If the lawyer collects personal data through the lawyer's website (e.g. using a contact form), the lawyer is required to publish on such website the basic information under Articles 13 and 14 of the GDPR. If the lawyer does not have a website, the information under Article 13 and 14 of the GDPR must be provided otherwise.

-

Example: The recommended practice for lawyers is to publish the information under Article 13 and 14 of the GDPR in the bottom bar of the web page as e.g. "Privacy Policy," "Protection of Privacy," or "Protection of Personal Data," etc. A reference to these policies may be used by the lawyer when collecting personal data (for example, when collecting consents), in contracts or within the signature in an email communication.

6.2.3 Privacy Policy template in Annex 2 below serves as a guidance for the fulfillment of the information obligation of lawyers pursuant to Article 13 and 14 of the GDPR in particular in relation to the data subjects who are their clients. However, by mandatory publication of such policy on their website, lawyers also make it more likely that it will be read by data subjects other than clients to whom the lawyer owes no obligation to provide such information. Privacy policy published on the lawyer's website should be sufficient for lawyers to meet obligations pursuant to Article 13 and 14 of the GDPR. This does not rule out that this obligation might be complied with otherwise. In cases where it is highly unlikely that data subject may become aware of the privacy policy on the lawyer's website (and the lawyer is under an obligation to inform them), the lawyer should also use other methods of providing basic information pursuant to Articles 13 and 14 of the GDPR.

Example: In such specific cases, the recommended practice for lawyers is to provide privacy policies to clients in printed forms, for example in the offices of the law firm or in correspondence or in person, especially if the client does not have access to the Internet.

6.2.4 To demonstrate the compliance with the obligation to inform data subjects in accordance with Article 13 of the GDPR, it is relevant whether the data subject has the opportunity to familiarise himself or herself with that information, and not whether the data subject actually did so because the data subject is not obliged to read or familiarise with this information. It is not necessary for the data subject to confirm the provision of basic information, for example by marking, consent, declaration or signature.

6.2.5 The timing for compliance with the information obligation under Article 13 of the GDPR is defined as the time when personal data are obtained. If certain lawyer's process takes longer (i.e. is not immediate) and collection of personal data is linked to that process, the lawyer should be able to comply with his or her information obligation under Article 13 of the GDPR at any time during this process. It is in the interest of the data

subject to have enough time to get acquainted with the information under Article 13 of the GDPR. Where, for instance, the data subject decides to conclude a contract for provision of legal services, it is sufficient if the data subject has the opportunity to become familiar with this basic information at any time during the process of conclusion of such contract, while he or she is present at the law firm or later by familiarising with documents sent to the data subject's email. The relevant factor is that the data subject had possibility to become acquainted with that information if he or she has such an interest. That the data subject has been informed of the existence and availability of that information while his or her personal data were collected and the data subject has decided not to familiarise with such information is not regarded as a violation of the lawyer's information duty. There is an exception to this obligation, if the data subject already has the information (for example, an amendment to a contract that changes the subject matter of the contract but the purpose and scope of the processing of personal data remains preserved). The lawyer must be able to prove this.

6.2.6 The timing for compliance with the information obligation under Article 14 of the GDPR is set later than under Article 13 of the GDPR. This information obligation can be complied with by the lawyer at the latest within one month, or earlier, at the time when the lawyer first communicated with the data subject or prior to first transfer of personal data to another recipient. Lawyers may comply with this information obligation by taking any option described above.

6.2.7 The lawyer is not required to provide information in cases and situations set forth in Article 14 (5) of the GDPR. During the exercise of legal profession, these cases and situations apply especially to individuals other than clients. For example, if personal data are collected from other natural persons under special legislation applicable to the lawyer (e.g. the Anti-Money Laundering Act, the Act on Legal profession, etc.), information about a counterparty or witness, the lawyer is not required to provide to such persons any information under Article 14 of the GDPR. The lawyer may also use, with respect to other natural persons, an argument that the personal data must remain confidentialunder the obligation of confidentiality that the lawyer owes to the client. If the lawyer provides some information under Article 14 of the GDPR (for example about the source of data about another natural person), this could lead to a breach of confidentiality obligation, such other natural person would learn the client's identity. This is without prejudice to further derogations provided for in Article 14 (5) of the GDPR. This paragraph is without prejudice to situations where the lawyer collects personal data directly from the data subject. In this case, Article 13 of the GDPR applies.

6.2.8 It is the recommended procedure for lawyers to refer to this Code in the document that the lawyer uses to comply with his or her information obligation pursuant to Articles 13 and 14 of the GDPR (e.g. Privacy Policy in Annex 2 below).

6.2.9 To promote transparency and informing the public about the processing of personal data by lawyers, the Slovak Bar Association will publish this Code on its website in its public Section accessible to all without the need to login.

6.3 Right to access personal data

6.3.1 Data subjects have the right of access under Article 15 of the GDPR, including the right of data subject to obtain from the lawyer a confirmation whether the lawyer is processing personal data about the data subject or not. Only when the lawyer processes personal data about data subject, the data subject is entitled to seek (in one request or in stages) other rights under the right of access, specifically:

i. right to obtain information pursuant to Article 15 (1) of the GDPR and 15 (2) of the GDPR (appropriate safeguards relating to the transfers of personal data to third countries pursuant to Article 46 of the GDPR);
ii. right to access the personal data processed by the lawyer;
iii. right to obtain a copy of processed personal data.

6.3.2 When providing information under Article 15 (1) and Article 15 (2) of the GDPR, lawyers are authorised to use the same manner and method of providing information as that which applies to the provision of information under Articles 13 and 14 of the GDPR. Information under Article 15 (1) of the GDPR should, however, be adapted to the circumstances surrounding the particular data subject.

Example: Provision of information under Article 15 (1) of the GDPR should be based on the fact that the data subject is already likely able to become aware of the privacy policy and is likely to request this generic information confirmed and adapted to him or her in a personal manner. The lawyer should respond in this way (e.g. should select from the list of all purposes only those purposes that are relevant in relation to such data subject).

6.3.3 The right of access is not an absolute right of the data subject and does not constitute the right to gain access

to the lawyer's internal systems or premises. The right of access is conditioned by the specific condition of the possibility of such access[14] and shall not have adverse consequences for the rights and freedoms of others.[15] "Other" may include, in particular, a client, but also a lawyer, other law firms belonging to a group of law firms and other data subjects or other persons than the data subject requesting the access.

Example: The data subject's access to personal data should be considered as impossible or unfavorable to the rights and freedoms of others, especially if prohibited by law or if it compromises the lawyer´s obligation to maintain confidentiality under the Act on Legal profession. This may be the case in particular if the lawyer, after a specific assessment of the situation, concludes that access is requested by a person other than the client without the consent of the client and at the same time that this could lead to a violation of the duty of the lawyer to maintain confidentiality under Section 23 of the Act on Legal Profession. However, the lawyer is required to carefully assess the situation.

6.3.4 The mere information that the lawyer processes personal data about a particular individual other than a client may have adverse consequences for the client, as it may hinder the legal preparation of the lawyer and the client, for example for filing a lawsuit. The mere information that the lawyer is processing personal data about a particular individual may be a violation of the lawyer's duty to maintain confidentiality because in the context of the situation it may be clear to another natural person that the processing relates to a particular client. If, for example, the lawyer should also confirm the source from which the personal data about such other natural person were obtained, by doing so the lawyer would probably have to confirm the identity of the client and so breach the duty of confidentiality.

Example: The lawyer protects the interests of the client and maintains confidentiality even by not confirming to other natural persons other than the client pursuant to Article 15 (1) of the GDPR that the lawyer processes personal data about them without the client's consent.

6.3.5 It is the particular feature of lawyer's duty to maintain confidentiality under Section 23 (3) of the Act on Legal Profession that the lawyer is also obliged to maintain confidentiality even if the client or all of the client's legal representatives release the lawyer from this obligation provided that the lawyer considers that the release from such confidentiality duty is to the detriment of the client. The lawyer enjoys a sovereign position with respect to assessing what is to the detriment of the client.

Example: If a natural person other than the client requests from the lawyer under Article 15 of the GDPR, even with the consent of the client, and the lawyer considers that allowing access would not be in the interest of the client, the lawyer would be obliged not to grant the other natural person access under Article 15 of the GDPR in spite of such client's consent.

6.3.6 The right to provide a copy of personal data under Article 15 (3) of the GDPR is a supplementary right of the data subject under the right of access. Where the right to provide information under Article 15 (1) of the GDPR is exercised, the lawyer will provide to the data subject only the categories of personal data that are processed with respect to specific data subject. Where the right to provide a copy of personal data pursuant to Article 15 (3) of the GDPR is exercised, the data subject exercises the right to be provided a specific "value" of such personal data (for instance: Jozef, 41). Copies of personal data need not be provided in any specific structured format. The right to obtain a copy does not mean that the lawyer is obliged to provide copies of documents or files. The right of access under Article 15 of the GDPR does not mean the access to the entire client file (even if the client holds such right - but not under GDPR).

Example: Where the lawyer provides the client with access to his or her personal data in the lawyer's office, when doing so the lawyer must pay attention to not put at risk the obligation of confidentiality that the lawyer owes to other clients (for instance, by making client files or other information visible or available). If the lawyer provides access to personal data to another natural person with the consent of the client, the lawyer does not provide to this person the entire client file for inspection, but only the information and documents containing the personal data of the data subject. The lawyer is entitled to remove (for example, to black out) information from these documents in order to maintain confidentiality vis-à-vis the client.

6.3.7 Given that the lawyer has more extensive information and documentation obligations to the client under the Act on Legal Profession, the Rules of Professional Conduct for lawyers and other professional regulations than under the GDPR, the lawyer responds to the affirmative in principle to all client's requests for information or documents, whether it is a request under Article 15 of the GDPR or not.
Example: According to Section 6 Rules of Professional Conduct for lawyers, the lawyer is obliged to a)

[14] Recital 63 of the GDPR: "***Where possible**, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.*"
[15] Recital 63 of the GDPR: "***That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software.***"

properly and in a timely manner inform the client how the lawyer proceeds with the handling of the case and send to the client all the documents from which the client derives rights and obligations unless otherwise agreed with the client in writing; b) handle carefully the documents the client has entrusted to the lawyer or the lawyer received on behalf of the client during the provision of the legal service; c) respond in writing to the written requests of the client related to the provision of legal services. Written information also includes communication by electronic or other technical means; in doing that the lawyer at the same time takes care to maintain the duty of confidentiality.

6.3.8 The lawyer is obliged to use the same response in the following cases:

- the lawyer does not process personal data that relates to the data subject;
- the lawyer processes personal data that relates to the data subject but for reasons stated above (mainly Sections 6.3.3, 6.3.4 a 6.3.5) the lawyer is not entitled to confirm this to the data subject due to potential breach of lawyer's duty to maintain confidentiality or the client's interests;

and the recommended response is as follows:

Example: Lawyers are not allowed to confirm to a natural person that they do not process personal data about him or her. The reason for this is that by doing so the lawyers could compromise their responses in case when they would be in fact processing the personal data related to a natural person but for reasons of maintaining confidentiality and client's interests they would be obliged not to confirm this. This means that we either do not process your personal data or process personal data about you but we are unable to confirm it. Accordingly, under the Code of Conduct of the Slovak Bar Association, lawyers use this template response for both situations. For reasons of law, we can neither provide you any further information under the GDPR. For more information, please refer to Section 6.3 of the Code of Conduct of the Slovak Bar Association available at www.sak.sk/kodex.

6.3.9 The response in Section 6.3.8 above does not apply to situations where the lawyer satisfies the right of access. The response under Section 6.3.8 above is covered by the general one month time limit with reference to Article 12 (4) of the GDPR.

6.3.10 If it is abundantly clear from the circumstances of a particular case that a natural person other than a client (e.g. a counterparty) already knows that the lawyer is processing personal data in connection with the particular client, for instance because judicial proceedings are already in progress or this is evident, for example because the lawyer in this case has already approached this natural person on behalf of the client, the lawyer takes the following recommended procedure:

Example:

- ***The lawyer in general responds affirmatively to the request of the data subject with regard to processing of his or her personal data under Article 15 (1) of the GDPR;***
- ***The lawyer is entitled to refuse the request for access or copy of personal data pursuant to Article 15 of the GDPR due to duty of maintaining confidentiality and protection of cleint's interests with reference to Section 18 (8) of the Act on Legal Profession;***
- ***With respect to other rights of the data subject, the lawyer proceeds according to the following points.***

6.4 Right to rectification, right to erasure ('right to be forgotten')

6.4.1 The data subject has the right to obtain from the lawyer the rectification of inaccurate personal data concerning him or her and has the right to have incomplete personal data completed, including by means of providing a supplementary statement. However, the lawyer as the controller is the one to determine whether the personal data are inaccurate in view of the purposes of their processing. The right to rectification under Article 16 of the GDPR must be interpreted in accordance with the principle of accuracy under this Code.

6.4.2 The right to erasure of personal data is mistakenly perceived by general public as an absolute right that can be used to achieve at any time the erasure of all personal data processed by the controller. The right to erasure is only applicable in the cases defined in Article 17 of the GDPR that are not general or absolute. The data subject should explain these reasons in his or her request and the lawyer should have the right to request the explanation if the data subject did not do so.

Example: If the data subject requests the lawyer to erase personal data without giving reasons for erasure under Article 17 of the GDPR (nor are the reasons clear from the context of such request), the lawyer has the right to respond (within a period of one month from the submission of the incomplete request) to the data

subject by requesting him or her to supplement the request with grounds on which the data subject requests the erasure. In this case, Section 6.1.4 above applies accordingly to the passing of the one month period.

6.4.3 Without prejudice to the above, the lawyer is entitled to refuse to act on the request for erasure of personal data if one of the grounds referred to in Article 17 (3) of the GDPR is applicable. Relevant to lawyers are in particular the grounds for refusal resulting from Article (3) (b), (d) and (e) of the GDPR, i.e: (i) the processing of personal data is necessary for compliance with the legal obligation of the lawyer; (ii) the processing of personal data is necessary for archiving purposes in the public interest; and (iii) the processing of personal data is necessary for the establishment, exercise or defence of legal claims (first and foremost, client's claims but these may also be lawyer's claims).

Example: The lawyer will not erase the personal data under the request of a data subject if:

- ***The retention period for the personal data for the purposes of practice of profession (provision of legal services), as established by the lawyer, continues to run;***
- ***The personal data are subject to pre-custody obligation under the Act on Archives (storage period + discarding procedure);***
- ***Professional regulations of the Slovak Bar Association require or recommend that such personal data be not erased or shredded;***
- ***Any claim to compensation for damage caused by the lawyer has not yet been statute-barred and the personal data are necessary for the establishment, exercise or defence of legal claims of the lawyer (even where the proceedings have not been initiated).***

6.4.4 Without prejudice to the above, the lawyer is entitled to refuse to act on basis of the request for erasure of personal data if the request is manifestly unfounded (Section 6.1.5 above).

6.5 Right to restriction of processing

The right to restriction of processing does not serve as a legal defense of other natural persons against the lawyer's clients or advice, and must be interpreted in this way. Fulfilment of conditions for the exercise of the right to restriction of processing is considered similarly as are considered the reasons for erasure of personal data explained above. The right to request restriction of processing of the personal data processed by the lawyer for the purpose of practice of the profession should be held only by the natural person who is the client or by another natural person with the consent of the client (if the lawyer considers that it is in the interest of the client).

6.6 Right to data portability

6.6.1 The data subject has the right to request the provision of personal data pursuant to Article 20 (1) of the GDPR only in relation to personal data that are processed by automated means (i.e. electronically); processed on the legal grounds of consent or performance of the contract (under Article 6 (1) (a) or (b) of the GDPR); and that were pro-actively provided to the lawyer by the data subject. These conditions will not be met in most cases in relation to the personal data of other natural person as the lawyer in most of these cases processes the personal data collected from the client.

6.6.2 The right to portability does not apply to the personal data that are processed by lawyers on legal grounds other than consent or performance of the contract.[16] Data categories that do not fall under the right of portability include, in particular, all personal data processed on a legal ground resulting from specific laws or legitimate interests as explained above. By default, this category also includes personal data about other natural persons as these the lawyers do not process on the ground of contract or consent.

6.6.3 As specific legislation may use the term 'consent' also with meanings other than that in the GDPR, the consent under Article 20 (1) of the GDPR means only a consent to the processing of personal data under Article 6 (1) (a) or Article 9 (2) (a) of the GDPR, but not any other type of consent.

6.6.4 The right to data portability must not adversely affect the rights and freedoms of others. Compliance with the request for dat aportability could have adverse consequences if by doing so the lawyer would provide personal data in conflict with the lawyer's duty of confidentiality, as is also covered in more detail in Section 18 (8) of the Act on Legal profession.

Example: In relation to personal data processed for the purpose of practice of the profession, the right to

[16] Recital 68 of the GDPR: *"It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties.* ***It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation*** *to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller."*

data portability applies only to those personal data that were directly provided in an electronic form by the client who is a natural person. The right to data portability does not belong to legal persons. The lawyer cannot allow the other natural persons to exercise the right to data portability without the client's consent in accordance with the provisions of Section 23 Act on Legal profession.

6.6.5 These data are most commonly provided in .doc, .docx, .rtf, .xls, .pdf, .jpg, .jepg, .png, .gif formats or in the body of an e-mail. If the lawyer is required to provide personal data under the right to data portability in a structured, commonly used and machine-readable format, the lawyer may provide personal data in the same format in which they were received from the client.

6.6.6 The right to data portability is without prejudice to obligations owed by lawyers to their clients with respect to providing information or documents.

6.7 Right to object

6.7.1 The data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing by lawyers of personal data concerning him or her which is based on legal ground of public interest or legitimate interest. Upon receipt of the request by the data subject, the lawyer is obliged, within the time limit under Article 12 GDPR, to demonstrate to the data subject the compelling legitimate reasons for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims. If the lawyer is unable to demonstrate these reasons for processing within the given time, the lawyer must not process the personal data starting on the moment when this period expires.

Example: If the lawyer uses a CCTV system to protect his or her legitimate interests (e.g. protection of property), the lawyer must be able to demonstrate that his or her legitimate interest is overriding if the data subject files an objection pursuant to Article 21 GDPR. The recommended procedure is to draft and have in connection with these purposes a written assessment of the legitimate interest.

6.7.2 The data subject have the right to object to the processing of personal data for the purposes of direct marketing. After the objection has been sent, lawyers must no longer process the personal data for the purposes of direct marketing, and after that the lawyers are obliged to terminate related processing operations within the time limit under Article 12 GDPR (without undue delay but not later than within one month).

6.8 Automated individual decision-making, including profiling

Although legal profession may, by its nature, have also adverse legal effects on other natural persons (such as on a counterparty), in the ordinary course of legal profession there is no automated individual decision-making under Article 22 GDPR. Lawyers should, however, always consider the possibility of automated individual decision-making whenever they make use of modern data processing technologies.

7 Data protection impact assessment and prior consultation

7.1 Data protection impact assessment

7.1.1 Data protection impact assessment is a specific obligation of lawyers in relation to certain types of processing of personal data that are likely to result in a high risk to the rights and freedoms of natural persons. The obligation to conduct a data protection impact assessment does not apply to all lawyers across the board and, within the meaning of GDPR recitals, lawyers practicing alone are partially exempted from this obligation (irrespective of the way in which they practice legal profession).

Example: Recital 91 GDPR: "The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory."

7.1.2 The data protection impact assessment could most often be relevant for law firms (companies) which, according to Article 35 (3) b) GDPR, process, on a large scale, personal data relating to criminal convictions and offences referred to in Article 10 GDPR. The law firm under the previous sentence is a law firm that:

a. specialises primarily in criminal law and income (sales) from advice in criminal law at least once in the last three years represented 70% of total income (sales) in the given financial year;
b. it is not a small firm under Section 12.1 below (i.e. the firm has more than 5 employees and a turnover of

more than 500,000 euros);

c. has pending criminal cases at least in six different districts of regional courts.

7.1.3 Data protection impact assessments may be relevant for lawyers in case they decide to depart from the recommendations given by the Slovak Bar Association regarding the use of software or cloud services with a storage facility located in the countries of the European Economic Area (EU + Iceland, Norway and Liechtenstein).

7.1.4 However, a checklist of situations that may be covered by the obligation to conduct data protection impact assessment can also result from guidelines or opinions of the Office for Personal Data Protection and does not necessarily concern only the practice of legal profession.

7.1.5 Lawyers may conduct one data protection impact assessment for similar or recurring situations and thus use the measures resulting from the conclusions of one data protection impact assessment for all similar situations. Lawyers are entitled to carry out the data protection impact assessment in any way that meets the requirements of Article 35 (7) GDPR.

7.2 Prior consultation with the Office for Personal Data Protection

Lawyers are required to request the Office for Personal Data Protection for prior consultation under Article 36 GDPR if such processing would result in a high risk in case that the lawyer does not take the measures to mitigate this risk.

8 Security of personal data

8.1 Adequacy of security measures

8.1.1 Crucial for the assessment whether personal data are protected by the lawyer at adequate level in compliance with GDPR is the assessment of adequacy of security measures taken in view of the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

8.1.2 The GDPR exemplifies the following security measures that can be used to demonstrate an adequate level of personal data security:

i. the pseudonymisation and encryption of personal data;

ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

iii. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

8.1.3 However, neither the circumstances for assessment of adequacy nor the examples of security measures given above mean that every lawyer must implement the same security measures. Application of GDPR principles may result in different security measures taken by different lawyers, taking into account their specific circumstances.

8.1.4 Some security measures are considered as standard, given the costs of implementation and the duty of a lawyer to maintain confidentiality. On every device the lawyer uses to process personal data:

- only properly licensed software must be installed;
- antivirus software must be installed (use of paid version is recommended);
- appropriate password security must be used (passwords must contain at least large and small characters and a number).

8.1.5 Lawyers are required to check if the software they use for data processing allows pseudonymization or encryption and, if so, they should use this functionality. Lawyers also need to take appropriate measures to physically protect office premises, and in particular the premises where client files or lawyer's servers are located.

8.1.6 When taking GDPR security measures, lawyers should follow the standards and recommendations issued by the Slovak Bar Association for the purchase of software and/or cloud services (the "**SBA Recommendations**").[17] SBA Recommendations provide, among other things, as follows:

Example: The Slovak Bar Association strictly does not recommend that lawyers use, in the practice of legal

[17] Available at https://www.sak.sk/blox/cms/sk/adv/electronic/cloud/id1/_event/open

profession, emails or storage services that provide free cloud services that are not safe, store data in locations that do not guarantee the required protection of personal data (outside EEA) and are the target of hackers and malware (such as Gmail, Google Drive, Hotmail, or OneDrive, iCloud or Dropbox). Employees must be properly instructed that in the performance of their work tasks they are prohibited from using their own emails or storage services under the previous sentence.

8.1.7 SBA Recommendations include, among other things, a 'cloud checklist' that contains data protection guidelines. This Code adds the following to those recommendations in the light of the GDPR:

Example: When deciding whether to use a cloud solution and deciding on the choice of cloud provider, lawyers should assess whether the cloud provider complies with a privacy-related Code of Conduct (if adopted). When choosing a provider, lawyers are reminded that they may entrust the processing of personal data to another processor only if such processor provides sufficient guarantees of GDPR compliance. If the cloud provider refuses to be treated as a processor, for example if it does not want to conclude a contract with the lawyer under Article 28 GDPR, this should be a sign that the provider does not provide sufficient guarantees.

8.1.8 When taking security measures according to the GDPR, lawyers may also follow relevant recommendations of the Council of Bars and Law Societies of Europe.[18]

8.2 Notification of a personal data breach to the Office for Personal Data Protection

8.2.1 Lawyers must, not later than 72 hours after having become aware of a personal data breach, notify the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The key for the start of this period is the moment when the lawyer verifies that a personal data breach has occurred and what risks it can pose to the rights and freedoms of natural persons, rather than a discovery that a personal data breach may have occurred. Lawyers are required to perform the verification under the preceding sentence without undue delay after finding that a personal data breach may have occurred. If the notification cannot be submitted within the given time period, a justification of delay should be inserted into the notification and information may be provided in several stages without any further undue delay.

Example: The lawyer loses his or her business laptop, client files or portable data carrier and, taking into account their content, considers that the loss of that information is likely to result in risks to the rights and freedoms of natural persons.

8.2.2 In accordance with Article 33 (5) GDPR, the lawyer must document each and every personal data breach, including the facts and circumstances relating to the personal data breach, its effects and the measures taken to address it.

Example: The lawyer may use the sample form provided in Annex 4 to document a personal data breach.

9 Data protection officer

9.1 Lawyer's data protection officer

Lawyers are obliged to designate a data protection officer only if conditions described in Article 37 GDPR are met. In general, the conditions pursuant to Articles 37 (1) a) and b) GDPR are not met during the ordinary practice of legal profession. For lawyers, the obligation to designate a data protection officer will apply in particular with reference to Article 37 (1) (c) GDPR where the lawyer's core activity is the processing, on a large scale, of personal data relating to criminal convictions and offences under Article 10 GDPR.

Example: If the lawyer considers that he or she should carry out a data protection impact assessment within the meaning of Section 7.1.2 of this Code, the lawyer will also have the obligation to designate a data protection officer. This is without prejudice to other circumstances requiring the designation of the data protection officer.

9.2 Lawyers as data protection officers

9.2.1 The lawyer is authorised to perform the function of data protection officer for his or her clients as part of practice of his or her profession (provision of legal services), either individually or in collaboration with other persons (if the data protection officer is a group or a team of persons). All tasks of the data protection officer under Article

[18] Available in English at: https://www.sak.sk/blox/cms/sk/sak/zahranicne/uzitocne/id2/id1/id1/_getFile

39 GDPR may but need not be performed by the lawyer as part of his or her provision of legal services.

Example: The client who is a legal person agrees with the lawyer on performance of the function of data protection officer and the client then reports the contact details of such lawyer as data protection officer to the Office for Personal Data Protection, as a result of which the lawyer becomes a contact point for the Office for Personal Data Protection, for example if there is an inspection. However, the client may agree that the data protection officer will be constituted of its internal IT employee, internal HR employee, and the lawyer. The data protection officer should have clearly defined status, roles and responsibilities relating to each member of the team, and in such case contact details to be published and reported may be also generic, such as dpo@firm.sk. The lawyer does not need to perform all tasks of the data protection officer to be a member of a data protection officer team. In that case, the data protection officer may act as a three-member panel and make decisions by a two-member majority, where each member may disagree with a decision, or otherwise.

9.2.2 Conclusion of a separate contract that will outline all details of performance of the function is a practice recommended by this Code for each case when the function of the data protection officer is performed by the lawyer.

9.2.3 That the lawyer is bound, within the limits of the law, by client's instructions if the lawyer exercises the function of the data protection officer does not mean that the lawyer does not comply with the requirements for position of the data protection officer under Article 38 (3) GDPR.[19] The GDPR and the Act on Legal Profession aim to retain the independence of the lawyer and the data protection officer. Lawyers can also interpret their independence through the CCBE Code of Conduct (Section 2.1):

Example: The many duties to which a lawyer is subject require his absolute independence, free from all other influence, especially such as may arise from his personal interests or external pressure. Such independence is as necessary to trust in the process of justice as the impartiality of the judge. A lawyer must therefore avoid any impairment of his independence and be careful not to compromise his professional standards in order to please his client, the court or third parties. This independence is necessary in non-contentious matters as well as in litigation. Advice given by a lawyer to his client has no value if it is given only to ingratiate himself, to serve his personal interests or in response to outside pressure.

9.2.4 If the lawyer, as th edata protection officer, receives an instruction from the client to respond to a request from the data subject, this does not mean to be an instruction under Article 38 (3) GDPR, as such instruction does not aim to limit the independence of the data protection officer, nor does it aim to limit the independence of the lawyer under Section 2 (2) of the Act on Legal Profession.

Example: An instruction that would undermine the independence of the lawyer and the data protection officer might be a client's instruction to change the negative opinion of the lawyer as a data protection officer. If the lawyer is convinced that the procedure as envisaged by the client is unlawful, the lawyer is required to maintain his or her independence and insist on such opinion despite the client's request.

9.2.5 The lawyer's suitability, seen from the perspective of data protection officer's independent status, is also due to lawyer's inability to receive a binding employment instruction from the client as well as to lawyer's possibility to withdraw from the contract with the client if the requisite trust between the lawyer and the client was broken or if the client's instruction is contrary to regulations of the Slovak Bar Association (including this Code).

9.3 Conflict of interest

9.3.1 In light of Article 38 (6) GDPR, the lawyer as the data protection officer may exercise also other tasks and duties in relation to the client, but the client must ensure that none of such tasks and duties results in a conflict of interests of the lawyer as the data protection officer. Although it is the client's obligation to ensure that the lawyer is not in a position of conflict of interest, lawyers should alert the clients to such potential conflict and actively avoid it.

9.3.2 The lawyer as the data protection officer will have no conflict of interests under Article 38 (6) GDPR if the lawyer provides to the client legal advice also in areas other than data protection.

Example: The lawyer performing the function of the data protection officer and, at the same time, the lawyer providing legal advice in commercial law to the same client is not in a situation of a conflict of interest under Article 38 (6) GDPR.

9.3.3 The lawyer as the data protection officer will have no conflict of interests under Article 38 (6) GDPR if the lawyer

[19] *"The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks."*

first provides to the client advice in personal data protection and then starts to perform the role of the data protection officer for that client, while the lawyer gives to that client no other advice than the exercise of tasks of the data protection officer in data protection.

Example: The lawyer who first prepares the client for the GDPR and subsequently starts to perform the function of the data protection officer for the same client is not in a situation of a conflict of interest under Article 38 (6) GDPR.

9.3.4 The lawyer as the data protection officer might have a conflict of interests under Article 38 (6) GDPR if the lawyer simultaneously provides to the client advice in data protection and performs the function of the data protection officer.

Example: There might be a conflict of interest if, for example, the lawyer, on the one hand, provides legal advice in the preparation of the client's contractual relationship with the processor in a manner that is based on acceptance of the risk of non-compliance with the GDPR (which is the client's right) and, on the other hand, the lawyer as the data protection officer would need to indicate the possible non-compliance with the GDPR when monitoring compliance with the GDPR where, moreover, the lawyer as the data protection officer should disqualify himself from such procedure. For this reason, lawyers should in principle either provide legal services in personal data protection or act as data protection officers but should not simultaneously perform both for the same client.

9.3.5 The GDPR does not imply that the data protection officer should give advice to data subjects. The lawyer as the data protection officer gives advice in principle only to the client and the client's employees. That data subjects may contact the data protection officer under Article 38 (4) GDPR has no effect on this. If the client is not obliged to respond to a data subject's request, neither the data protection officer has this obligation. The lawyer might always be contacted by the client's counterparty but that this might happen does not mean that the lawyer must respond.

9.3.6 The data protection officer is obliged to co-operate with the Office for Personal Data Protection. This obligation also applies to the client under Article 31 GDPR. The obligation of co-operation does not imply that the data protection officer is obliged to report to the Office for Personal Data Protection all deficiencies under the GDPR learned by such officer during the performance of his or her duties. The co-operation with the supervisory authority means that the client and the data protection officer will not unlawfully prevent the supervisory authority from performing its tasks. It is legitimate for the data protection officer, similarly to the lawyer, to protect and promote the interests of the client (and not those of the data subject or the Office for Personal Data Protection).

10 Professional ethics and the GDPR

10.1 The lawyer acts in the practice of legal profession so as not to demean the dignity of the lawyer's profession. To this end, the lawyer is obliged to observe the rules of professional ethics and other rules determined by professional regulations of the Slovak Bar Association. Before a lawyer initiates, in his or her own case, legal or similar proceedings against another lawyer, such lawyer is obliged to use the conciliation procedure before the bodies of the Slovak Bar Association for the sake of respect and honour of the legal profession.

10.2 The GDPR should not be used as a tool in competition between lawyers. If it is established that the lawyer or lawyer's employees or other persons authorised by the lawyer exercised their right of data subjects under the GDPR against another lawyer with an aim to cause harm, hinder or prevent such other lawyer from practicing legal profession, this conduct may constitute a breach of rules of lawyer's professional ethics. Any suspicion of such conduct must be reported by lawyers to the Slovak Bar Association.

11 Monitoring mechanisms

11.1 Monitoring of compliance with this Code under Article 41 GDPR and Section 87 of the Act on Personal Data Protection may be requested only by the Slovak Bar Association or other entity with its express written consent. Due to duty of confidentiality, lawyers are not required to be subjected to such entity's monitoring unless the conditions under the previous sentence are met.

11.2 It is the duty of each lawyer to comply with the laws and internal professional regulations of the Slovak Bar Association. The mechanisms for monitoring the compliance with this Code are therefore already set out in the Act on Legal Profession, Rules of Professional Conduct for Lawyers and the Disciplinary Code but may also be

regulated in other specific rules and regulations that pertain to the monitoring of compliance with this Code.

11.3 Oversight over compliance with any professional regulations of the Slovak Bar Association is vested with the supervision commission, disciplinary commission, disciplinary panels and appelate disciplinary panels of the Slovak Bar Association. Under Section 23 (6) of the Act on Legal Profession, the lawyer cannot invoke the duty of confidentiality during the disciplinary proceedings.

11.4 Lawyer's rights and obligations during the performance of monitoring the compliance with the adopted Code are governed, in particular, by the provisions of Section 2 (7) and (11) Disciplinary Code that provide as follows:

"Disciplinary accused has the right to:
a) appoint a representative; such representative may be only a lawyer who is not a member of the elected body of the Bar;
b) comment on the proposal, inspect the disciplinary file and make excerpts from it;
c) file a bias objection against the disciplinary panel or member of the disciplinary panel;
d) attend at the hearing of the matter before a disciplinary panel, make statements about the action that constitutes the subject-matter of disciplinary proceeding, propose taking of evidence, ask questions, comment on evidence taken and experts and, at the conclusion of the hearing, comment on issues of facts and law of the deliberated matter;
e) appeal against the decision of the disciplinary panel;
f) file a motion for reversal of valid and effective disciplinary decision;
g) lodge an application for the annulment of disciplinary measure and deletion from the register of disciplinary measures;
h) lodge a motion with the court for review of valid and effective decision."

"The lawyer against whom a complaint is made is obliged to file a response to the complaint."

11.5 General rules for disciplinary proceedings are set forth mainly in Sections 56 to 60 of the Act on Legal Profession and further explained in the Disciplinary Code. Section 57 (7) of the Act on Legal Profession reads: "*Unless this Act or disciplinary code of the Bar internal rules directly regulate some practices and procedures in the disciplinary proceeding or the position, rights and obligations of the parties to disciplinary proceeding, the provisions of a separate legal rule shall apply accordingly (footnote: Code of Criminal Procedure).*"

11.6 In excess of what is given above, anyone may turn to the Slovak Bar Association with a request to provide an interpretation of this Code, by electronic means at gdpr@sak.sk. Every year, the Slovak Bar Association will issue and publish a report on the compliance with this Code for the past calendar year, based on survey among lawyers, events, requests received at the above email address or suggestions made by the lawyers.

12 Adequate documentation of lawyers under the GDPR

12.1 This Code should contribute, under Article 40 (1) GDPR, to the correct application of the GDPR, taking into account the specific features of the different processing sectors and the specific needs of micro, small and medium-sized enterprises. For this reason, the Code differentiates between lawyers using well-established EU Commission's methodology and inserts another definition for the legal profession sector (the "**Small Firm**"):[20]

Enterprise category	Headcount	Annual turnover	Balance sheet total
Medium-sized enterprise	Less than 250	Less than 50 mil. €	Less than 43 mil. €
Small enterprise	Less than 50	Less than 10 mil. €	Less than 43 mil. €
Micro enterprise	Less than 10	Less than 2 mil. €	Less than 2 mil. €
Small firm	Less than 5	Less than 500,000 €	Less than 500,000 €

12.2 If the lawyer is a small or medium-sized enterprise, the lawyer is obliged to adopt adequate internal policies for the protection of personal data pursuant to Article 24 (2) GDPR regardless of any other circumstances.

12.3 If the lawyer qualifies as a micro enterprise or a small firm, the lawyer is not automatically required to adopt internal data protection policy pursuant to this Code. In such case, the lawyer will adopt an internal data protection policy only if it is appropriate taking into account the processing activities of the lawyer pursuant to Article 24 (2) GDPR.

[20] Guidelines of EU Commission to definition of SME availible at https://ec.europa.eu/docsroom/documents/15582/attachments/1/translations/sk/renditions/native

12.4 When developing the internal data protection policy, the lawyer will take appropriate procedure according to Internal Data Protection Policy Requirements set out in Annex 3 below. The internal data protection policy must reflect the reality.

12.5 The recommended procedure with regard to documenting GDPR compliance is to collect and store all documentation related to data protection in the same file or storage facility under the title "**Documentation of compliance with GDPR**".

Example: Among other things, Documentation of compliance with GDPR may, taking into account the needs, preferences and circumstances of a particular case, include the following:

- ***lawyer's internal data protection policy, if adopted; if an internal data protection policy is not adopted and the lawyer is a micro enterprise, the lawyer should have documented reasons leading him or her not to adopt the above tool (as explained above);***
- ***most recent lawyer's privacy policy published on his or her website and provided on client's request in printed form;***
- ***this Code;***
- ***records of processing activities pursuant to Article 30 GDPR (a similar obligation already had been in place with regard to lawyers under prior legislation – see record sheets);***
- ***sample internal form for documenting a security incident, where such sample form is given in Annex 4 below;***
- ***assessment of legitimate interest where legitimate interests pursued by the lawyer or third party override the interests, interests, rights and freedoms of data subjects if the lawyer relies on the legal ground of legitimate interest pursuant to Article 6 (1)(f) GDPR;***
- ***records of employee training in personal data protection;***
- ***received and cleared requests made by data subjects;***
- ***documentation of security measures taken, including potential analysis of impact on the rights and freedoms of data subjects;***
- ***sample contracts or contracts with processors, joint controllers, data protection officer or other contracts related to e.g. cross-border flows of personal data;***
- ***documented instructions to processors (if instructions do not form part of the contract);***
- ***instructions to employees pursuant to Article 29 GDPR (general instructions can be demonstrated by written instructions from employees);***
- ***records of communication with processors relating to verification of GDPR compliance;***
- ***other information and documentation related to data protection.***

13 Final provisions

13.1 This Code was drafted in compliance with the GDPR and specific legislation, where strictly necessary.

13.2 Annexes are an integral part of this Code. Each reference to this Code includes a reference to its Annexes.

13.3 This Code and all relationships arising therefrom will be governed by the laws of the Slovak Republic.

13.4 For the purpose of this Code, capitalised terms or abbreviations have the meaning given in Annex 1. All terms defined in the GDPR whenever used in this Code are used in the same meaning unless expressly provided otherwise in this Code. In the case of any discrepancies, this Code takes precedence. Unless the context requires otherwise, the words in the singular also import the plural and vice versa.

Annex1
Definitions

For the purpose of this Code, capitalised terms or abbreviations have the following meanings:

Act on Accounting means Act no. 431/2002 Coll. on accounting as amended;

Act on Legal Profession means Act No. 586/2003 Coll. on the Legal Profession and on Amending Act No. 455/1991 Coll. on the Business and Self-Employment Services (Business Licensing Act) as amended

Act on Archives means Act no. 395/2002 Coll. on archives and records retention, as amended;

Act on Personal Data Protection means Act no. 18/2018 Coll. on protection of personal data;

Rules of Professional Conduct for Lawyers mean the Rules of Professional Conduct for Lawyers of the Slovak Bar Association, as adopted by the General Assembly of lawyers on 10 June 2017;

Anti-Money Laundering Act means Act no. 297/2008 Coll. on protection against the legalisation of crime proceeds and on protection against terrorism financing and on amendment of certain laws, as amended;

Code of Civil Non-Contentious Procedure means Act no. 161/2015 Coll., Code of Civil Non-Contentious Procedure, as amended;

Civil Code means Act no. 40/1964 Coll., the Civil Code, as mended;

Code of Civil Contentious Procedure means Act no. 160/2015 Coll., Code of Civil Contentious Procedure, as amended;

Commercial Code means Act no. 513/1991 Coll., the Commercial Code, as amended;

Criminal Code means Act no. 300/2005 Coll., the Criminal Code, as amended;

Code of Criminal Procedure means Act no. 301/2005 Coll., Code of Criminal Procedure, as amended;

Code means this Code of Conduct for Processing of Personal Data by Lawyers;

Disciplinary Code means the Code of Disciplinary Procedure of the Slovak Bar Association, as adopted by the General Assembly of lawyers on 10 June 2017;

GDPR means EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation);

Labour Code means Act no. 311/2001 Coll., the Labour Code, as amended;

Office for Personal Data Protection means the Office for Personal Data Protection of the Slovak Republic;

Public Sector Partners Act means Act no. 315/2016 Coll. on register of public sector partners, as amended.

Annex 2
Privacy Policy

Protection of personal data of our clients and other natural persons is important for us. This Privacy Policy provides an explanation how we process personal data when providing legal services at **[business name]** with registered seat at: [X], Identification number (IČO): [X] (hereinafter referred to as "**we**" or "**us**"). If you have any questions or queries you may contact us by phone on [X], by sending an e-mail to privacy@office.sk or by post at the registered seat.

[If the lawyer designates the data protection officer:] In our law firm, the Data Protection Officer has been designated who is your contact point for answering any questions relating to the protection of personal data or the handling of requests made by data subjects. The contact details of the Data Protection Officer are: [X].

In the processing of personal data, we are primarily governed by the EU General Data Protection Regulation ("**GDPR**"), which also governs your rights as the data subject[21] the provisions of the Act on Personal Data Protection applicable to us (in particular Section 78), the Act on Legal Profession (Section 18) as well as other applicable legislation. We are in compliance with the Code of Conduct adopted by the Slovak Bar Association ("**SBA**") that explains processing of personal data by lawyers. You can familiarize yourself with the SBA's Code of Conduct in more detail at www.sak.sk/gdpr.

Why we process personal data?

- Processing of personal data is necessary for us mainly to:
- provide legal services to our clients and pursue the legal profession;
- comply with various legal, professional and contractual obligations; and
- protect legitimate interests of us, our clients and other persons.

What are our purposes of processing personal data and on what legal grounds are they made?

Purpose	Legal ground	Relevant legislation
[fill]	**[fill]**	**[fill]**

What are our legitimate interests that we pursue?

[Only if the lawyer relies on legitimate interests (e.g. protection of premises by CCTV system).]

Who are recipients of our personal data?

We provide personal data of our clients and other natural persons only to the extent necessary and always while maintaining the confidentiality of the data recipient, e.g. to our employees, persons authorised to take individual legal actions within provision of legal services, substituting or cooperating lawyers, **[other offices belonging to our group],** our accountancy advisors **[our professional advisors e.g. auditors],** the Slovak Bar Association (e.g. in the case of disciplinary proceedings) or to providers of software or the support to our law firm, including employees of those persons.

Although our obligation to provide your personal data to public authorities is limited for reasons of confidentiality, we are required to frustrate the commission of criminal offences and we also have the obligation to report information regarding prevention of money laundering and terrorism financing.

[In case of joint controllers, lawyers should explain in this part at least fundamental parts of their joint controllers agreement pursuant to Article 26 of the GDPR]

What countries we transfer your personal data to?

[21] See articles 12 to 22 of the GDPR: http://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:32016R0679&from=EN

We do not intend to transfer your personal data outside the EU and/or European Economic Area. **[We use safe cloud services of a verified provider with servers located in an EU jurisdiction.]**

What automated individual decision making we pursue?

[Only applicable if lawyer conducts processing pursuant to Article of the 22 GDPR]

How long do we store your personal data?

We store personal data as long as is necessary for the purposes for which personal data are processed. When storing personal data, we follow the recommended retention periods under the Resolution of Council of Slovak Bar Association no. 29/11/2011, e.g.

- The incoming mail book / register and the outgoing mail book / register, after it has been filled, is kept by the lawyer for ten years from the date of receipt or sending of the last mail registered in such book;
- The inventory list is archived by the lawyer for ten years after made;
- If the lawyer keeps a list of client names and client records electronically, at the end of the calendar year he or she will make its printed form for the calendar year and store it in the office without any time limit;
- Client files shredding period is 10 years and starts to run on the day when all the conditions for deposition of the file to the archive are fulfilled.

Lawyers are subject to professional regulations of the Slovak Bar Association that interpret their obligations under the Act on Legal Profession, according to which there are certain circumstances that extend our retention periods of personal data and explicitly prevent us from shredding some documents on reasonable grounds, such as:

- A client file that contains original documents delivered to us by the client cannot be shredded;
- It is not possible to shred client file protocols and list of client file names;
- It is not possible to shred the client file or its part that the lawyer is obliged to submit to the state archives;
- It is not possible to shred the client file if any proceedings before the courts, state administration bodies, law enforcement authorities, the Slovak Bar Association are pending that have a material relation to the contents of the client file or that concer the lawyer's legal action or omission in providing legal services in that client's matter.

How we collect your personal data?

If you are our client, we often obtain your personal data directly from you. In that case, obtaining your personal data is voluntary. Depending on the particular case, the failure to provide personal data by clients may affect our ability to provide high-quality legal services or, in exceptional cases, may give rise to our obligation to refuse to provide legal services. Personal data about our clients may also be obtained from publicly available sources, from public authorities or from other third parties.

If you are not our client, we often obtain your personal data from our clients or from other public or statutory sources by making requests to public authorities, through extracts from public registers, obtaining evidence in favour of our client, etc. In such a case, we may obtain personal data without your knowledge and against your will on the basis of our statutory authorization and the obligation to practice law in accordance with the Act on Legal Profession.

What rights do you have?

"If we process personal data based on your consent, you have the right to withdraw your consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal."

"You have a right to object to any processing that is based on legitimate interest or public interest as well as to any direct marketing purposes including profiling."

As a client, you have the right to request access to your personal data and request their rectification. When processing personal data during the provision of legal services, you have no right, as a client or any other natural person (e.g. a counterparty), to object to such processing under Article 22 of the GDPR. If personal data relate to a client (regardless of whether the client is a legal or natural person) other persons do not have the right of access to such data or the right to data portability, due to our legal obligation to maintain confidentiality with reference to Article 15 (4) of the GDPR, Article 20 (4) of the GDPR and Section 18 (8) of the Act on Legal profession: "A lawyer is not obliged to provide

information on the personal data processing, facilitate access or enable data portability pursuant special legal regulation *(footnote: Article 14 (5) (d) 15 (4) and Article 20 (4)* of the *GDPR)* if it may lead to breach of professional duty of secrecy in compliance with this Act."

Cookies [Only if the lawyer process cookies on the website]

Cookies are small text files that improve website usage, e.g. by allowing us to recognise previous visitors when logging in to a user environment, remembering a user's choice when opening a new window, measuring website traffic, or evaluating usage of the website for improvement. Our website uses cookies for the purposes of **[please insert]**. You can always stop storing these files on your device in the settings of your web browser. Setting your browser is considered, under Section 55 (5) of the Act on Electronic Communications, as your consent to the use of cookies on our site.

Changes to this Privacy Policy

Protection of your data is not a one-time issue for us. The information we give you with regard to processing of personal data may change or cease to be up to date. For these reasons, we may change this Privacy Policy at any time and to any extent. If we change this Privacy Policy substantially, we will bring such changes to your attention, for example through a general notice posed on this website or by explicit notice delivered by email.

Annex 3
Internal data protection policy requirements

Introduction

The purpose of internal policy on the protection of personal data is to ensure, in an organisational and practical way, that the lawyer is in compliance with obligations derived from the GDPR and is prepared and capable of assessing and handling requests of data subjects in compliance with the timeframe and in accordance with the GDPR. The internal data protection policy is also a tool for managing data protection agenda in the organisation, serving as a division of tasks and responsibilities in this area, as well as setting out other policies and rules relating to the protection of personal data. Lawyer's internal policy must correspond to reality and its compliance must be regularly evaluated. The content of the internal policy must be appropriate to processing operations performed by the lawyer. The recommended procedure is to adopt the internal policy as part of rules for work under the Labor Code.

Basic internal data protection policy requirements

The lawyer's internal policy can address the following areas:

1. Division of tasks and responsibilities in data protection

a. Who is entitled to take a decision (e.g. respond to a data subject's request, report a security incident, etc.)?
b. Who is responsible for preparing the documents for deciding on and evaluating an application / request?
c. Who is to be informed internally about the course and outcome of a particular task?
d. What are alternative roles in case of unavailability of a particular person?
e. Who has the right to intervene in this process?
f. Is it possible for a lawyer to categorise and define different processes and tasks in personal data protection beforehand, or is it possible to set only general responsibility?
g. Who is responsible for information security issues in the organisation?
h. Who is responsible for supervising and coordinating the data protection agenda?

2. Procedure for handling the requests made by data subjects

a. Who receives the request and evaluates its content according to the GDPR?
b. What is the next step after such evaluation?
c. Who is informed that the fact that a request has arrived?
d. How is each request registered and marked (does the lawyer have a ticketing system for assignment of tasks)?
e. Who oversees this process (data protection officer)?
f. What are the time periods for each step?
g. Who prepares the draft of the final answer?
h. Who is obliged to provide co-operation to whom?
i. Who receives the final decision on the response?
j. Who is responsible for responding?
k. Is it possible to prepare template responses? (note: some template responses are already hinted at in the body of the Code)

3. Procedure of notification of personal data breaches

a. Which security incident detection techniques are used by the lawyer?
b. Who will assess the detected personal data breach? On what basis such assessment will be made?
c. Who and how will ensure the processes related to reporting of personal data breaches to the Office and data subjects?
d. What are the processes related to the lessons learned from a security incident and the effectiveness of an internal system for protecting personal data (e.g. by complementing and / or enhancing appropriate technical and organisational security measures)?

4. Designation, status and tasks of data protection officer

a. Who will act as the data protection officer?
b. Does this person have a guaranteed independence in a sufficiently independent manner to fulfill his or her statutory tasks?
c. Is there a conflict of interest taking into account status and functions of the data protection officer?
d. Are tasks and responsibilities of the person authorised to perform the function of data protection officer defined sufficiently internally?
e. Does the data protection officer prepare annual reports on the condition of data protection?

5. General principles of care with regard to information assets

a. Has the lawyer classified his or her information assets that are important for the processing of personal data?
b. Has the lawyer classified information according to their degree of sensitivity to him or her and also to the client in the event when their security is compromised by an unauthorised person?
c. Are the most sensitive information and personal data protected under heightened organisational and technical security measures?
d. Is the back-up of important information and personal data secured in an appropriate way?
e. What is the security in cases and situations when third parties access our assets?

6. Access & Password Policy

a. It is essential for "everyone to have access to everything"? – how can the lawyer effectively ensure that the extent of the processing of personal data in relation to specific employees is minimised?
b. Are there different roles with different access privileges?
c. Who decides on the allocation of roles and access permissions? On what basis?
d. Is it possible to prove these decisions on granting access rights in a formal way (e.g. by issuing authorisations and instructions for the data recipient)?
e. Is it possible to effectively remove access rights and user permissions, and check their proper removal (for example, change and termination of employment)?
f. What are the password requirements and how often do passwords change?
g. What is the procedure for change of password?

7. Use Policy

a. Are rules in place for use of Internet, wifi, mobile devices, computers, files, notes, specific programs, e-mail, social networks, etc.?
b. Is it allowed to use your own devices for work purposes?
c. Is it allowed to use work devices for private purposes?
d. Are there rules in place for the use of easily portable media or material carrier of electronic data (e.g. USB key, external HDD, CD / DVD) (e.g. the obligation to encrypt data, the obligation not to aggregate sensitive information and personal data on these media, insertion of third party media into your own devices, etc.)?

8. Principles of communication

a. Sending encrypted or password-protected documents to clients with a password / key sent by different communication channels such as via text message (SMS)?
b. Using email communication encryption?
c. What are the things that employees cannot communicate about when they are not in the office with respect to the obligation of confidentiality and protection of personal data?
d. What means can employees use to communicate with each other and with clients (can they use Whatsapp, Facebook messenger, social media, etc.)?
e. Keeping the communication with the client as recommended by the SBA in recommendations for file-keeping;
f. What is it that lawyer's employees are obliged to report and to whom (suspected security incident or personal data breach)?

9. Principles of manipulation with hard copies

a. Is it allowed to, and is a special regulation in place with regard to, taking files from protected office premises (e.g. for home study, attendance at a hearing, filings with authorities made in person, etc.)?
b. Is the "clean desk" policy in relation to employees adopted?
c. Are unnecessary and / or damaged documents containing sensitive information and personal data shredded without delay?

10. Principles of selection of choice of suppliers with possibility of access to data

a. Is the differentiation of suppliers properly set in terms of their position under substantive personal data protection law (controller / processor)?
b. Depending on the nature of the supplier, did we enter into proper contracts with processors or issue appropriate authorisations and instructions for each type of data recipient, if possible and appropriate?
c. Do we adequately commit our internal staff to duty of confidentiality?
d. Have we established processes and rules for evaluating suppliers to verify their ability to provide sufficient security for the processing of personal data and compliance with mandatory obligations in the field of personal data protection (e.g. audits, defined requirements for basic standards, etc.)?
e. Are our main contractual relationships with suppliers drafted so that we can easily terminate cooperation in cases of inadequate protection of personal data?

f. Is there a part of internal policy that covers cleaning service providers? Do they have access to all documentation? Is the risk adressed?

11. Internal procedures of monitoring, workshops and education

a. Does the lawyer perform internal audits on compliance with adopted organizational and technical security measures?
b. Does the lawyer perform subsequent internal audits in cases of identifying a personal data breach?
c. Are mechanisms of monitoring by the lawyer put in place in a transparent and proportionate manner, and are modern IT tools for information protection as well as legalised employer control mechanisms (e.g. DLP - Data Loss Prevention software solutions) used?
d. Does the lawyer perform regular staff training on internal policies, security measures taken, and real threats with potential to compromise sensitive information, with an emphasis on specifics of the profession?
e. Does the lawyer mainly provide induction trainings for new employees who have not previously worked in legal profession?

12. Retention of personal data and erasure procedures

a. Is compliance with the recommendation of the Slovak Bar Association in connection with client file management ensured?
b. Can the lawyer determine what documents cannot be shredded? Are these documents labelled?
c. Can the lawyer determine at any time when and what personal data must be erased?
d. Are various stages of personal data retention, from their collection to their erasure, defined?
e. Is there a designated person and procedure for technically reliable (irreversible) erasure of data?

13. Confidentiality

a. It is a recommended procedure to formally instruct and bind all employees of the lawyer to maintain confidentiality under the Act on Legal Profession as well as under the Act on Personal Data Protection;
b. Employee duty to notify the lawyer all breaches or suspected breaches of duty of confidentiality.

Annex 4
Sample form for documenting a personal data breach

This record on personal data breach was drafted in compliance with Article 33 (5) of the GDPR[22] and serves to document the breach and file the security measures and procedures to mitigate the risk for the rights and freedoms of natural persons (hereinafter referred to as the "**Record**").

Company / Lawyer:
Registered seat:
Identification number (IČO):
Registered:
Contact:
(hereinafter referred to as the "**Controller**")

Whereas:

(A) According to Article 4 (12) of the GDPR: "personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (hereinafter referred to as the "Breach").

(B) According to Article 33 (5) of the GDPR: "The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."

The Controller has decided to document the Breach as follows:

1.	**Date, location and time of finding of Breach and internal identification of Breach:**	[please insert date, location and exact time when the Breach was found; it is also recommend to number or otherwise identify individual records on Breaches]
2.	**Contact of DPO, if designated:**	[please insert title, name, surname, email and phone number]
3.	**Contact of IP consultant or IT department:**	[please insert title, name, surname, email and phone number]
4.	**Contact of other persons with significant knowledge of the Breach:**	[e.g. internal employee who contacted the DPO regarding the Breach]
5.	**Basic description of the Breach:**	[please provide in your own words what actually happened]
6.	**How the Breach was found:**	[missing documents or files, automatic notification from the security software, notifying unusual network activity phenomena, logging data analysis notification, employee report, reporting to an IT consultant, notification from a processor, DPO's activity, mediation, receiving suspicious e-mail, receiving a cyber request for a ransom attack, failure of online service functionality due to a Ddos attack, knowledge learned as a result of applying employer's control mechamisms to employees, etc.]
7.	**Description of the nature of the Breach:**	[description of a specific event that has been identified and that has the potential to put at risk or violate the integrity, confidentiality, or availability of information that contains personal data. The event that has led to accidental or unlawful destruction, loss, alteration, unauthorised provision of personal data or unauthorised access to information containing personal data should also always accurately characterised. At the same time, the list of data subjects affected by security incident and their (estimated) number and the list of data potentially compromised personal data that are processed, and indication nof quantity of compromised or corrupted data (such as by number of records and data size in MB, GB, TB)]
8.	**Identification of security measures taken to prevent the occurrence of the Breach:**	[please specify the security measures and procedures that were under internal policies, guidelines or security projects intended to ensure the protection against occurrence of the Breach detected]

[22] Article 35 (5) of the GDPR: **"The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."**

9.	**Possible causes for the occurrence of the Breach:**	[in the case of a Breach that actually results in a risk and/or high risk for the rights and freedoms of natural persons, Controller's internal investigation and control will aim to identify the causes of the Breach, describing all relevant facts that had an effect on the occurrence, progress and impacts of the Breach detected] [it is also recommended to provide a chronological description of incident's progress, description of threats that have been made, identification of vulnerabilities that have been used and how it all took place; it is also advisable to list assets affected by the Breach, identify and define the security measures that were broken where the Breach occurred in spite of taking of adequate security measure and indicate the presumed reason why the security measure was broken] [it is also recommended to record what specific security measures or practices have been violated if there is a causal link between the occurrence of the Breach and such violation of measures of practices, and try to identify the person or persons responsible for breach of obligations and internal rules in connection with the Breach]
10.	**Relationship of the Breach and residual risk for the rights and freedoms of natural persons:**	[please provide considerations about the nature of the Breach with respect to residual risks and uncovered risks that the lawyer has documented, for example in his or her security project under the previous legislation]
11.	**Description of the likely consequences of the Breach:**	[please describe identified and potential negative effects of the Breach on the lawyer and lawyer's assets and also on the duty of confidentiality, the persons whom the personal data in question concerned, the legitimate interests of the client]
12.	**Description of measures taken or proposed to address the Breach:**	[lawyer to indicate all actions that were taken or that are proposed to be taken in specific time by specific authorised personnel with the aim to address the Breach]
13.	**Description of measures intended to mitigate the adverse effects of the Breach:**	[lawyer to indicate all actions that were taken or that are proposed to be taken in specific time by specific authorised personnel with the aim to mitigate the adverse effects of the Breach]
14.	**Proposed updates to security measures:**	[lawyer to document what steps have been taken to prevent similar incidents as the Breach from occurring in the future]
15.	**Assessment whether obligation arose to notify the data protection authority pursuant to Article 33 GDPR:**	[lawyer to answer the question: Is the Breach likely to result in a risk for the rights and freedoms of natural persons? and provide justification]
16.	**Assessment whether obligation arose to notify the data protection authority pursuant to Article 34 GDPR:**	[lawyer to answer the question: Is the Breach likely to result in a high risk for the rights and freedoms of natural persons? and provide justification. Please refer to Section 8.3 Code – lawyer should communicate the Breach under Article 34 of the GDPR only to clients and employees but not to other natural persons]
17.	**Date and time when the Breach was notified to the Office for Personal Data Protection:**	[please indicate the exact date and time of the notification and enclose a written proof that the notification was made - to be completed only if]
18.	**Reasons for missing the deadline for notification of the Breach to the Office for Personal Data Protection:**	[please give reason for failure to comply with the period of 72 hours (3 days) - to be filled in only if the obligation to notify was established and the deadline was missed]
19.	**Date, time and manner of communication of the Breach to data subjects:**	[please provide the exact date and time when, and manner how, the Breach was communicated to data subjects shall be stated – please refer to Section 8.3 Code – the lawyer should communicate the Breach under Article 34 of the GDPR only to clients and employees but not to other natural persons]
20.	**Position of Controller's statutory body on the Breach and next steps:**	[the statutory body to give its views on the above and approve the next steps (in particular, the decision to notify / not notify the Breach)]

Following the above documentation, the Controller has decided:

❑	to not notify the personal data breach to the Office for Personal Data Protection of the Slovak Republic pursuant to Article 33 of the GDPR (in this case, the Breach is documented only by this record);	*"because the Breach is **unlikely to result in a risk** to the rights and freedoms of natural persons "*
❑	to not notify personal data breach to the Office for Personal Data Protection of the Slovak Republic pursuant to Article 33 of the GDPR (in this case, the notification of breach will be appended to this record);	*"because the Breach **is likely to result in a risk** to the rights and freedoms of natural persons "*
❑	to communicate the Breach also to data subjects pursuant to Article 34 of the GDPR;	*"because the Breach **is likely to result in a high risk** to the rights and freedoms of natural persons "*
❑	to not communicate the Breach to data subjects pursuant to Article 34 of the GDPR;	*"because the Breach **is unlikely to result in a high risk** to the rights and freedoms of natural persons "*

Drafted by:
Approved by:
Date:

Annexes (if relevant):

- Copy of the notification of Breach to the Office for Personal Data Protection;
- Copy of the communication of Breach to data subjects.


Slovenská
advokátska
komora