

PRIVACY POLICY

Effective date: 01.07.2019.

Please, revise carefully this Privacy Policy before the disclosure of your personal data. This Privacy Policy includes all information related to the data processing activity of KassaiLaw concerning the collection, use, storage, disclosure and erasure of data (with special attention to personal data), in line with Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter referred to as the GDPR), and with Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as "Infotv.")

This Privacy Policy explains how KassaiLaw handles and treats your data when you

- (i) visit our site, www.kassailaw.com (the "Site") or
- (ii) engage with KassaiLaw to use the products or services that the firm provides (our "Services").

It also includes information about individuals whose personal information we may process as a result of providing the Services to third parties and individuals who apply to work at KassaiLaw.

1. Preamble

- 1.1. KassaiLaw (hereinafter referred to as the '**Controller**') is operated by Kassai Karola Law Firm (registered seat: 1126 Budapest, Németsvölgyi út 54/a.), a law firm registered at the Budapest Bar Association in Hungary, providing legal and other client services. In the course of this activity, Controller may carry out activities related to controlling or processing personal data of those affected (hereinafter referred to as the '**Client**' or '**Data Subject**'); hence, in order to ensure the compliance with the respective laws and regulations, the Controller has resolved on the formulation of this Privacy Policy concerning the external aspects of data controlling and processing.
- 1.2. For the purposes of this Privacy Policy, the terms 'we' or 'our' etc. shall mean the Controller.
- 1.3. This Privacy Policy requires the expressed consent hereto by the Clients; such consent may be withdrawn at any time.
- 1.4. The Controller shall be responsible for the formulation of this Privacy Policy, for the observance and making the persons falling under the scope hereof to observe these provisions, for the enforcement, updating and amending of this Privacy Policy. The Controller may amend this Privacy Policy unilaterally, at any time. Certain business processes and development require the later enhancement of the sphere of the purposes of data processing. The Controller hereby undertakes to proceed in strict compliance with the provisions of the GDPR and Infotv. in any case that requires the processing of personal data. This Policy shall come into effect upon its publication. The prevailing version of this Policy is available on the website: www.kassailaw.com
- 1.5. The Controller ensures for every Data Subject the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any personal data processing, the possible consequences of such processing and the scope of information that may be given to the Data Subject. 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. However, the result of those considerations should not be a complete refusal by the Controller to provide all information to the Data Subject.
- 1.6. The expressed consent to this Privacy Policy shall be voluntarily, specific and based on the related information; only such consent may serve as a basis of processing of the Client's personal data. The consent shall cover all processing activities carried out for the same purpose or purposes.
- 1.7. The Controller is committed to the protection of the Clients' personal data and places special emphasis on the observance of informational self-determination rights; hence, it undertakes to handle the personal data of Clients confidentially and to take the safety, technical and organizational measures that guarantees the security of data.
- 1.8. The Controller shall process the personal data lawfully, fairly and in a transparent manner; the collection of data is allowed only for specifically defined, unambiguous and lawful purposes and the scope of the collected data is limited to those suitable and relevant from the aspect of the purposes of data processing and necessary for the achievement thereof.
- 1.9. In the course of data processing, the Controller shall attempt to ensure the accuracy and up-to-date nature of the personal data; therefore, it shall take all necessary measures for the immediate erasure or rectification of the data that are inaccurate from the aspect of the purposes of the processing.

- 1.10.Regarding that the registered seat of the Controller is in Hungary, the provision of administrative protection in connection with the personal data processing defined in this Privacy Policy is the competence of Nemzeti Adatvédelmi és Információbiztonsági Hatóság ('NAIH', Hungarian National Authority for Data Protection and Freedom of Information). See Sec. 11.2. for contact details to NAIH.

2. Service provider's data

Name of Controller	KassaiLaw
Registered seat of Controller	HU-1126 Budapest, Németvölgyi út 54/a.
The address of the customer service	-
The contact details of Controller, its electronic mailing address used for regular communication with customers	office@kassailaw.com
Phone number	+36-30241 6577
Website	www.kassailaw.com
The language of the contract	Hungarian and English

3. Applicable laws

The Controller hereby declares to process the personal data of data subjects (who are not (yet) in contractual relationship with the Controller), as well as its contractual partners in compliance with the prevailing laws and regulations, with special regard to the following:

- The related EU regulation: the General Data Protection Regulation of the European Union (Regulation 2016/679 (EU), the 'GDPR')
- Article VI of the Fundamental Law of Hungary
- Act CXII of 2011 on Informational Self-Determination and the Freedom of Information (Information Act)
- Act V of 2013 on the Civil Code (Civil Code)
- Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services (Electronic Commerce Act)
- Act CLV of 1997 on Consumer Protection (Consumer Protection Act)
- Act C of 2003 on Electronic Communications (Electronic Communications Act)

4. Legal Ground for Data Processing

- 4.1. The legal ground for personal data processing is the voluntary consent of the Client given thereto in knowledge of this information (Article 6 (1)(a) of the GDPR).
- 4.2. The Controller is entitled to the processing of the Clients' data on the basis of the contract concluded by and between the Controller and the User, in line with the purpose of such contract, for the sake of contractual performance (Article 6(1)(b) of the GDPR).
- 4.3. The processing of the personal data may be required for the performance of the Controller's legal obligations, like auditing and accounting liabilities (Article 6(1)(c) of GDPR).
- 4.4. The processing of the personal data may be required for the enforcement of the legitimate interest of the Controller or a third party (Article 6(1)(f) of GDPR).
- 4.5. The User shall grant his/her consent to the use of his/her personal data for advertisement purposes.

5. The Data Processed by KassaiLaw

- 5.1. We may collect personal information from you in the course of our business, including through your use of our Site, when you contact or request information from us, when you engage our legal or other services or as a result of your relationship with one or more of our staff or clients.
- 5.2. Whenever the Controller requests the Client to provide personal data, the Client may reject to comply with such request; however, in this case, the Controller is entitled to lawfully reject the provision of Services, hence, the Client may forfeit the use thereof. In case of any doubt, Controller may request Clients to verify their identities, copy their ID cards, which can be refused by Data Subject in any case, however in which cases Controller cannot guarantee the requested

information or service. The data subject explicitly consents to this data processing by Controller to the extent and for the time required for the purpose.

5.3. Within the scope of data processing, the Controller is entitled in particular to pursue the following activities: to collect, record, register, systematize, store and use the personal data for the purposes of data processing, to query, block, erase and destruct the data and to prevent the further use thereof.

5.4. Our primary goal in collecting personal information from you is to help us:

- verify your identity
- deliver our Services
- improve, develop and market new Services
- carry out requests made by you on the Site or in relation to our Services
- investigate or settle inquiries or disputes
- comply with any applicable law, court order, other judicial process, or the requirements of a regulator
- enforce our agreements with you
- protect the rights, property or safety of us or third parties, including our other clients and users of the Site or our Services
- with recruitment purposes, and
- use as otherwise required or permitted by law.

5.5. To undertake these goals we may process the following personal information:

Data Subject	Legal grounds	Data category	Purpose of Data Processing
Visitor on the Site	4.1.	Name Email address Other information relevant to the provision of Services.	Identification of the user and ensuring the communication, Establishment and maintenance of a reliable and safe environment, enforcement of claims and rights, prevention and handling of fraud, Conducting the complaint management process, carrying out a request
Individual Client in receipt of our Services or prospective individual Client	4.1. 4.2. 4.3.	Name, Contact information including email, phone number, Payment information, Information that you provide to us as part of us providing the Services to you, which depends on the nature of your instructions to KassaiLaw, Other information relevant to provision of Services.	Conclusion, amendment and performance of the contract, Maintenance and development of service Identification of the user and ensuring the communication, Establishment and maintenance of a reliable and safe environment, enforcement of claims and rights, prevention and handling of fraud.
Potential recruit, job applicant	4.1.	Name (first and last name)	Conclusion, amendment and performance of the legal relationship; employment, Identification of the applicant and ensuring the communication, Establishment and maintenance of a reliable and safe environment,

			enforcement of claims and rights, prevention and handling of fraud.
		Email address	Conclusion, amendment and performance of the legal relationship; employment, Identification of the applicant and ensuring the communication, Establishment and maintenance of a reliable and safe environment, enforcement of claims and rights, prevention and handling of fraud.
		Telephone	Identification of the applicant and ensuring the communication,
		Other data provided voluntary in the CV	Conducting the professional selection process
Employee, contributors	4.2. 4.3.	Name (first and last name)	Performance of the contract Compliance with legal obligations relating to employment (e.g. reporting to the necessary authorities)
		E-mail address	Performance of the contract Identification of the applicant and ensuring the communication
		Telephone	Identification of the applicant and ensuring the communication,
		Mother's name	Performance of the contract
		Address and post address	Compliance with legal obligations relating to employment (e.g. informing necessary authorities)
		Tax number	
		Social security number	
Bank account number, bank account details			
Compliant, requestor	4.1. 4.3.	Name (first and last name)	Conducting the complaint management process, carrying out a request Identification of the user and ensuring the communication
		E-mail address	Conducting the complaint management process, carrying out a request Identification of the user and ensuring the communication
		Phone number	Conducting the complaint management process, carrying out a request Identification of the user and ensuring the communication
		Address	Conducting the complaint management process, carrying out a request Identification of the user and ensuring the communication

5.6. KassaiLaw is primarily engaged by corporate entities and as such those instructors are not data subjects. However, as part of such instructions personal information may be provided to us (e.g. personal information relating to any of our corporate clients' or prospective clients' officers or personnel, any opponent or vendor or purchaser or personal information relating to their legal advisors or personnel, as relevant or similar).

- 5.7. The Data Subject may exercise his/her right to the restriction of data processing, to rectification or erasure of data and the right to object with respect to the data listed in Section 5.5. herein at any time, free of charge. For this purpose, the Controller shall ensure the possibility of electronic submission of the related requests to the following e-mail address: office@kassailaw.com. If such a request is submitted, the Controller shall respond to the Data Subject without undue delay, but in any case, within 25 days from the receipt of the request. Should the Controller reject to perform the request, it shall provide a proper justification of rejection.
- 5.8. Sensitive data necessary for the performance of the Contract
- 5.5.1. Controller does not control or process any sensitive data under any circumstances.
- 5.9. Automatic collection of data
- 5.9.1. If the Client does not expressly provide the Controller with his/her personal data and information in line with the provisions of this Privacy Policy, the Controller may not collect or process any personal data of the User in a way that would enable the identification of his/her person. We do not collect data of Users automatically, nor do we process any data automatically.
- 5.10. Data collected from third parties
- 5.10.1. The provision of data collected by Controller from third parties with respect to the Client and the data transfer towards the Controller the expressed consent of the Client is required, to be given directly to the third party in possession of all relevant information. Granting his/her consent shall be the responsibility of the Client and is not supervised by any means by the Service Provider; furthermore, the Service Provider is not liable for the collection and processing of such data by third parties. The transfer of the collected data towards the Service Provider shall be expressly allowed by the User on the surfaces of the concerned third party.
- 5.10.2. The services of third parties: if the User uses the services of a third-party service provider (like Facebook) in relation to getting access to Controller's Services, the Service Provider shall be entitled to request from the concerned third party the data of the User that are essential to the provision of the Services. To the provision or change of such data, the privacy policies of the concerned third-party service provider shall apply.
- 5.11. Cookies applied by the Controller
- 5.11.1. If the Client does not expressly provide the Controller with his/her personal data and information, the Controller may not collect or process any personal data of the Client in a way that would enable the identification of his/her person.
- 5.11.2. Cookies are short text files comprising of data related to the Client, sent by the browser to the hard disc of the Client's computer or mobile device. Such data are those of the Client's computer or device, generated in the course of the use of the Website and recorded by the cookies automatically in the course of technical processes. The automatically recorded data are automatically logged by the system upon visiting or leaving an application, without any statement or action of the User.
- 5.11.3. By visiting the Website, the Users consent to the use of session-type cookies by the Controller in relation to the Website, which are (in the sole consideration of the Controller) explicitly needed to browse through the Website and to use the functions thereof (e.g. recording of operations performed by visitor). The validity of such cookies is limited to the current visit of the user; such cookies are automatically deleted from the computer upon the end of the working session or by closing the browser.
- 5.11.4. The Controller uses only the cookies of third parties (e.g. Google).
- 5.11.5. The advertisements of the Controller are displayed on various websites on the Internet by external service providers (Google, Facebook). These external service providers (Google, Facebook) store the data of previous visits of the User on the Controller's Website by means of cookies, that allows them to display personalized advertisements for the User (so-called remarketing activity).
- 5.11.6. To the data processing activities of such external service providers the provisions of their data policies shall apply. The Controller's liability for such data processing is explicitly excluded.
- 5.11.7. The use of technologies mentioned hereinabove: the data collected by means of the above technologies may not be used for the identification of the User and these data may not be connected by the Controller to any other data that are suitable for such identification purposes.
- 5.11.8. The primary purpose of such data is the proper operation of the Website by the Controller, that requires the follow-up of visitors' data and filtering out of any eventual misuse.

5.11.9. In addition to the above, the Controller may use such information to analyse the tendencies of use, to develop and improve the functions of the Website and to get comprehensive traffic data of the entire use thereof. The information acquired this way may be used by the Controller to set up statistics, to prepare analyses, to transfer such statistical data that are unsuitable for the identification of visitors (like the number of visitors, the most popular subjects and contents) to third parties or to publish them in a summarized, anonymized form.

5.11.10. **Possibility to disable cookies:** is the User objects to the collection of his/her data by the Controller in connection with the use of the Website, he/she may **fully or partially disable the use of the cookies** among the settings of the browser or amend the message settings of the cookies; however, this may result in a more difficult use of the Website, what the User hereby expressly acknowledges and accepts.

6. The method and term of the use of the data collected

6.1. Processing of personal data by the Controller is allowed only if being essential, suitable for and limited to the extent and duration required to the achievement of the purposes set for processing.

6.2. In lack of a related legal obligation, the Controller will not publish, coordinate or connect the personal data with each other.

Purpose of Data Processing	Justification of purpose	Duration of data processing
The conclusion, amendment and performance of the contract	The Controller uses the data collected by them or through third party providers for the following purposes to conclude, amend and perform contracts. The personal data collected in the course of the use of the Services are to facilitate and enable the performance of the transaction required by the User. The Controller shall use the personal data of the User to enable the establishment of the contractual background for the provision of the services ordered by the User and to facilitate the completion of the contract.	The Controller shall process the personal data during the term of the contractual relationship or in case a contractual relationship has not been established, until the purpose of processing has ceased, or erases them in case further processing of such data is no longer necessary for the purpose of processing. User may request for the erasure of his/her data in a letter sent to the Office@kassailaw.com e-mail address. For the purposes of evidencing in the case of a dispute, the data of the concerned User shall be processed during the term of the general limitation period (5 years), and for five (5) years after the final and binding closure of the dispute, or will be preserved for 10 years after erasure set out in Infotv., if relevant (Infotv. Section 25/F (4)).
Maintenance and development of service	The Controller shall use the data collected by it or through third-party service provider for the following purposes of maintenance and development of service. The personal data collected in the course of the use of the Services are to facilitate the performance and to enable the updating of the transaction required by the User. The Controller shall use the personal data of the User to enable the continuous development and improvement of the Services.	
Identification of the user and ensuring the communication	The Controller may use the User's personal data to ensure effective communication with the User, in the course of which Controller contacts and identifies user through their contact data provided.	
Establishment and maintenance of a reliable and safe environment, enforcement of claims and rights, prevention and handling of fraud	The Controller may use the personal data of the User to secure the legitimate interests of Users in the course of the use of Services. In the scope of the above, the Controller shall be entitled to the following activities: the prevention and termination of fraud, spam, misuses and other harmful activities, to perform security	

	investigations and risk analysis, to check and verify the data provided by the user.	
Conduction of complaint management procedure	Documentation and verification of the conduct of the procedure, the actual examination.	The Controller shall process the personal data concerned until the purpose of processing has ceased, or erases them in case further processing of such data is no longer necessary for the purpose of processing. The data shall be stored for 5 years according to consumer protection rules, or will be preserved for 10 years after erasure set out in Infotv., if relevant (Infotv. Section 25/F (4)).
Third party data provided by a contractual partner in its own management	Actual performance of operating activities, operation of specific softwares	Competence of Partner. Controller does not store the data separately after they have been deleted from each system by the Partner.
Compliance with legal obligations relating to employment (e.g. informing necessary authorities)	Compliance with relevant informational, reporting obligations and obligations connected to taxation, contributions, etc.	Controller processes the data for 5 years starting from the last day of the calendar year in which employment ends, with the prohibition to discard labor, wage and social security records. Otherwise the limitation period in labor law is 3 years.

7. The persons having access to the data processed, data transfers

- 7.1. In order to ensure the undisturbed provision of the Services, the transfer of certain data to third parties may be necessary; the Data Subject shall be informed of such transfer in every case. In line with the prevailing laws and regulations, the Controller, its employees and subcontractors (eg. the accounting firm) shall have access to the personal data.
- 7.2. In order to ensure the proper provision of the services and for quality assurance purposes, as well as to enable the investigation of customer claims and complaints, the Controller may transfer the personal data within its company group. By the acceptance of this Privacy Policy, the consent of the Client to such data transfer shall be deemed given.
- 7.3. Data transfer shall take place solely if the Controller is able to justify the purpose and legal basis of transmission. Personal data must be transmitted solely to the extent necessary to achieve the purpose, taking into account the principles of rationality and proportionality.
- 7.4. Data transfer may take place in the following cases:

Recipient of data transfer	Scope of data that may be transferred
Transfer of data to employees	To the personal data processed by us, the Controller shall have access; the personal data shall also be made available to the employees of the Controller, but only if their access to and processing of personal data is required for the purposes of data processing related to the given data category.
Publicly displayable information	The Controller may only display publicly those information with respect to which the Data Subject has granted its consent to the disclosure thereof on the social/public surfaces of the Controller's Partners.
Compliance with Laws	Except for the cases defined in this section 7 and the case if the Controller is instructed by the court to transfer data upon provisions prescribing

	mandatory data transfer to a specific authority, state or administrative organ and such instruction cannot be lawfully rejected, the Controller may not transfer the personal data provided to it to third parties.
--	---

- 7.5. The Controller has no liability under any circumstances for the data processing activity of third parties (e.g. Google, Facebook, etc.); to these activities the privacy policies of the concerned service providers shall apply.
- 7.6. The Data Processor assists Controller in the smooth operation of the IT infrastructure that facilitates the storage of personal data provided to Controller, Data Processor has no direct access to personal data. The Controller hereby expressly declares that it has no direct or indirect liability with respect to the data processing activity of the Data Processor and the security of personal data in the course thereof; in this regard, the privacy policies and regulations of the Data Processor shall apply.
- 7.7. The Controller hereby reserves the right to involve further data processors to the processing, of which fact the Clients shall be notified by the amendment of this Policy.
- 7.8. Otherwise, the personal data of Users are not transferred to any third party by the Controller.

8. Rights and obligations of the Parties

8.1. Processing of Users' data, rights of information

- 8.1.1. The Data Subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. The Controller tries to maintain the accuracy and the up-to-date status of the personal data; notwithstanding the above, the Data Subject shall notify the Service Provider of any change in his/her data, at office@kassailaw.com. The Data Subject shall be responsible for ensuring the up-to-date status of the personal data.
- 8.1.2. Shall Data Subject decide to contact Controller with any request related to any of their rights under this chapter, they shall do so by completing the Written Complaint Submission Sheet which is part of the Request and Complaint Management Policy that forms Annex 1 to this Policy. After completion, the Complaint Sheet shall be signed and sent to Controller by post or email.
- 8.1.3. The Controller shall implement adequate measures in order to be able to provide the Data Subject with all information and notice related to data processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Information will be provided by the Controller primarily through its mail address office@kassailaw.com in writing, or via phone (+36-30/241-65-77) verbally; furthermore, such information may be requested directly at the registered seat of the Controller. Information may only be given after the verification of the Data Subject's personality.
- 8.1.4. The Controller shall provide to the Data Subject information on the actions taken upon his/her request without undue delay, but in any event within 25 days of receipt of such request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Controller shall inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay.
- 8.1.5. If the Controller does not take action on the request of the Data Subject, the Controller shall inform the Data Subject without delay, but at the latest within one month of receipt of the request of the reasons for not taking any action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.
- 8.1.6. The first request is free of charge. The second and all additional requests repeatedly filed are HUF 5,000, if the request is related to the same subject or subject matter in the ongoing year, the request is not for information purposes and the Controller legally disregards the rectification, erasure or restriction of the personal data handled on the basis of the repeated application. If a repeated request is justified because the act giving rise to the request has been caused by omission or activity attributable to the Controller, Controller may waive the charges set out.
- 8.1.7. Where the Controller processes a large quantity of information concerning the Data Subject, the Controller may request the Data Subject to specify the information or processing activities to which the request relates before the information is delivered.

8.2. Access

8.2.1. The Controller shall use all reasonable measures to verify the identity of a Data Subject who requests access, in particular in the context of online services and online identifiers. The Controller may not retain personal data for the sole purpose of being able to react to potential requests.

8.3. Rectification and erasure

8.3.1. The Data Subject is entitled to have the personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes the provisions of the related laws and regulations.

8.3.2. In particular, the Data Subject is entitled to have his/her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are originally processed.

8.4. Withdrawal of consent and restriction of processing

8.4.1. The Data Subject is entitled to withdraw his/her consent given previously to the processing of his/her data.

8.4.2. However, the further retention of the personal data is considered to be lawful where it is necessary for the protection of exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest etc. The processing of personal data is essential until the proper, contractual completion of the contract concluded by and between the Controller and the Data Subject.

8.5. Right to object

8.5.1. Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, the Data Subject shall, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation.

8.6. Right to data portability

8.6.1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller if the relevant legal conditions are met. However, Controller hereby informs Data Subject that it does not perform automatic data processing

8.7. The Obligation of the Data Subject

8.7.1. The User may only provide his/her personal data in the course of using the services; he/she shall declare the quality (lawfulness, reality and accuracy) of the data under criminal liability. If the data source provides another person's data, the consent of the actual data subject shall be acquired by the data source. If the Controller is concerned about the quality of the data provided, it may request the Client to verify such data. If the Client rejects to perform the Controller's request for verification, or the Controller, in its sole discretion, declares the data unlawful, unreal or inaccurate, the processing of such data may not be continued, and the Controller may reject to provide the Services.

8.7.2. The Controller shall have no liability, either direct or indirect, for the legal consequences arising from the fact that the User provided another person's data or provided false data, even if the Controller requested for the verification thereof.

8.8. Data Subject acknowledges the fact that requests towards exercising his or her rights set out in sections 8.3-8.6 may result in failure of the data processing purposes, which may eventually result in failure to perform the Service. Personal data cannot be erased in cases where Controller must comply with its legal obligation to retain and store said data. Controller shall inform the Data Subject at all times, duly justified, if the fulfilment of the data subject's request is not possible.

9. Further Important Information

9.1. Records of data processing activities

Service Provider complies with the obligation of keeping records of the data processing activities and maintains a record of data processing activities that is relevant to employment activities.

9.2. Data Protection Officer

In our standpoint, the Service Provider is not obliged to appoint a data protection officer, as the main activities of the Controller do not involve data processing operations that would allow a regular, systematic and high-scale follow-up monitoring of the Data Subjects; furthermore, the Controller does not process the special categories of personal data.

9.3. Supervisory organs and other authorities

The territorial scope of this Privacy Policy may cover also foreign authorities, if the Client has a registered seat or business site out of Hungary, in a foreign country.

9.4. Automated decision making, profiling

The Controller hereby declares that it applies no decision-making procedures that are based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Should the Controller apply such procedures in the future, the data subjects shall be properly notified thereof, and their consents will be requested.

9.5. Processing of sensitive data

The Controller hereby declares that it processes no personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Should the Controller process such sensitive data, this activity shall be pursued with special care and diligence, it may only process the sensitive data to the extent it is required.

The Controller hereby declares that processes no personal 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 data concerning a natural person's sex life or sexual orientation.

10. Personal data breach

10.1. In case of personal data breach, if the where the incident is likely to pose a high risk to the rights and freedoms of those concerned, we submit the report towards the data protection supervisory authority required by the laws and regulations, without undue delay, but in any case, within 72 hours from getting aware of the incident. We have developed internal procedures in case of personal data breach, and personal data breaches are also recorded into a registry. The data subjects affected by such personal data breach will also be notified, if the prevailing laws and regulations require so.

10.2. Should a threat of personal data breach be detected by Data Subject, we ask to report it immediately to Controller with the help of the Personal Data Breach Report Form that forms a part of the Personal Data Breach Management Policy (Appendix 2) on the office@kassailaw.com email address. Detailed rules for our applicable process in case of personal data breach can be found in our Personal Data Breach Management Policy.

11. Handling of complaints, data protection supervisory authority

11.1. In case of any request or complaint by Data Subjects regarding our personal data processing activities, we provide the opportunity to report them on any of the following contacts: in person, written: at the registered seat of Controller, telephone: +36-30/241-65-77 or email: office@kassailaw.com. Our Request and Complaint Management Policy (Appendix 1) sets out our processes for handling complaints, and contains a Written Complaint Submission Sheet, which may be sent to Controller by post or email after completion.

11.2. In case of being injured by the data processing practices of the Controller, the Data Subject shall have the right to file a complaint with the competent supervisory organ:

National Authority for Data Protection and Freedom of Information

Website: <http://naih.hu>

Mailing address: H-1530 Budapest, Pf.: 5.

Email: ugyfelszolgalat@naih.hu

Phone number: +36(1)391-1400

11.3. Furthermore, in case of personal data breach, you may initiate a court case before the Budapest Capital Regional Court against the Controller.

12. Changes of the Privacy Policy

12.1. The Service Provider reserves the right to amend this Privacy Policy at any time. Amendments will be published immediately on the website www.forshapp.com

12.2. In case of amendment, the Data Subject will be notified thereof thirty (30) days prior to the date of effectiveness of amendment, via e-mail or through the web page.

12.3. In case the Data Subject objects to such amendment, he/she may notify the Controller thereof and disclose his/her respective comments and notices via e-mail office@kassailaw.com furthermore, he/she may request the erasure of his/her personal data.

[Annex1: Personal Data Breach Management Policy](#)

[Annex2: Request and Complaint Management Policy](#)