



Privacy Policy

regarding data processing activities by SBGK Attorneys at Law

Identification of the Controller and legal background of the processings

SBGK Ügyvédi Iroda (hereinafter referred to as: “Controller”)

Postal address: H-1062 Budapest, Andrásy út 113.

Email: privacy@sbgk.hu

The processing shall be primarily governed by the following legislative acts:

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

Attorneys Act Act LXXVIII of 2017 on the Attorneys

Anti-Money Laundering Act Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing

1. Data processing related to establishing contact

Purpose of the processing If the customer contacts the Controller in email or by phone, and then for the Controller to be able to contact the customer and consult with him or her regarding a meeting in person.

Scope of the data processed The Controller processes the natural person customer’s name, email address, phone number, and in specific cases, additional personal data provided by the customer in relation to establishing contact or his or her case.

If the data subject establishes contact on behalf of a legal person, the processing shall also cover the data subject's name, company contact details (phone number, email) and the name of the company at which the data subject works. If the customer also discloses to the Controller the personal data of other data subjects (e.g. employees or former employees) in relation to the case presented by him or her, the processing shall also cover these personal data.

Legal basis of the processing The legal basis of the processing is the natural person customer’s consent [Article 6(1)(a) of the GDPR].

If the data subject is acting on behalf of a legal person, the legal basis of the processing is the Controller’s legitimate interest [Article 6(1)(f) of the GDPR].



The Controller's legitimate interest is in consulting with the data subject regarding the date of a meeting in person, thereby making it possible for the data subject to present the case to the Controller and being informed by the Controller preliminarily regarding the content of the legislation and the possible legal tools and solutions.

Term of the processing

If no further processing takes place other than contact, the Controller will process the personal data for 3 years.

2. Processing related to the offer

Purpose of the processing

The purpose of the processing is for the Controller to make an offer to the customer for the conclusion of the agency, with regard to the content of the contract and the agency fee.

Scope of the data processed

The Controller processes the natural person customer's name, email address, phone number, and in specific cases, additional personal data provided by the customer in relation to establishing contact or his or her case.

If the data subject establishes contact on behalf of a legal person, the processing shall also cover the data subject's name, company contact details (phone number, email) and the name of the company at which the data subject works. If the customer also discloses to the Controller the personal data of other data subjects (e.g. employees or former employees) in relation to the case presented by him or her, the processing shall also cover these personal data.

Legal basis of the processing

If the Controller makes an offer to a natural person, the legal basis is the preparation for the conclusion of the contract [Article 6(1)(b) of the GDPR]. If the customer does not provide the personal data necessary for preparing the offer to the Controller, the Controller will be unable to make an offer to the customer.

If the Controller makes an offer to a legal person, the legal basis for processing is the legitimate interest of the Data Controller [Article 6(1)(f) GDPR]. The legitimate interest of the Data Controller is to make an offer in relation to the matter presented by the customer .

Term of the processing

The term of the processing related to the offer is 5 years. The reason for retaining the data is to ensure that authentic evidence is available in the event any dispute arises as to the conclusion or content of the contract, the period during which the offer is binding, or the interpretation or validity of the contract.

3. Customer identification (customer due diligence) obligation and making of copies of instruments

Purpose of the processing

If an agency contract is concluded between the customer and the Controller, then prior to the conclusion of the contract, the Controller is required to perform



customer identification in order to promote the security of legal transactions and to reduce the chance of fraud, money laundering and other criminal offences.

This includes the event where during the term of the agency contract, the Controller obtains information regarding that the earlier customer identification (customer due diligence) was not appropriate, and consequently it needs to be performed again.

Legal basis of the processing

The legal basis of the processing is compliance with the Controller's legal obligation [Article 6(1)(c) of the GDPR]. The processing is required pursuant to Section 32 of the Attorneys Act and Section 73(1) of the Anti-Money Laundering Act. With regard to the making of copies of instruments, Section 7(8) constitutes the legal basis of the processing. The conditions of the processing are set out primarily in Sections 32-33 of the Attorneys Act and Sections 6-7, 11, 56-58 and 73 of the Anti-Money Laundering Act.

The cooperation in the customer identification (customer due diligence) is based on a legal obligation. If the customer fails to cooperate during the customer identification (customer due diligence), the Controller will not conclude an agency contract with the customer, or may terminate the contract.

Cases where customer due diligence is mandatory

Pursuant to Section 73(1) of the Anti-Money Laundering Act, customer due diligence is mandatory in the case of the following attorney activities:

- management of deposited funds and assets,
- transfer of ownership (share) in a company or other business organisation,
- transfer of ownership of real property,
- foundation, operation and termination of a company or other business organisation,
- unilateral declaration regarding the conclusion of trusteeship contract or trusteeship,
- transfer of movable assets (in particular, funds and financial instruments) for no consideration.

The process of customer identification and customer due diligence

The Controller identifies the customer, the customer's agent, the person with right of disposal and the representative.

The Controller requires the following instruments to be presented for the purpose of the certifying check of identity and the customer due diligence:

- for a Hungarian citizen, the personal identification document and the certificate certifying the home address,
- for a foreign citizen, the travel document or personal identification document, provided that it entitles the holder to reside in Hungary, the document certifying the right to residence or the document providing the right to residence,



- for a customer that is a legal person or unincorporated organisation, the foregoing documents of the person entitled to act on its behalf or upon its agency.

In the course of the identification, the Controller shall record the data specified in Section 32(3) of the Attorneys Act and Sections 7-9 of the Anti-Money Laundering Act, and may query them from the different public registries (such as the registry of personal data and addresses or the registry of driving licenses).

Scope of the data processed

The processing covers the following personal data:

- name (abbreviated name),
- citizenship,
- place and date of birth,
- mother’s name,
- home address (or address of residence),
- type and number of identification document,
- a copy of the identification document,
- signature.

Term of the processing

The Controller shall retain the data for 8 years from the date of fulfilment of the agency, or in the case of a long-term agency, from the date of termination of the business relationship.

In the case of an inquiry from the authority or the bar association, the Controller shall retain the data for 10 years from the date of fulfilment of the agency, or in the case of a long-term agency, from the date of termination of the business relationship.

Possible recipients of the processing

In the course of the processing, primarily (but not exclusively) the Controller may transmit personal data to the following recipients:

- if the Controller becomes aware of any fact, data or circumstance suggesting money laundering, the Controller will make a report to the Budapest Bar Association,
- the Anti-Money Laundering Information Unit of the National Tax and Customs Administration may submit inquiries to the Controller in the scope of the performance of its tasks,
- in the event of an audit conducted by the Bar Association, to the Bar Association proceeding in the case, for the purpose of certifying compliance with the rules governing the activity of attorneys.

4. Identification of the beneficial owner

Purpose of the processing

If an agency contract is concluded between the customer and the Controller, then prior to the conclusion of the contract, the Controller is required to identify



the beneficial owner in order to promote the security of legal transactions and to reduce the chance of fraud, money laundering and other criminal offences.

This includes the event where during the term of the agency contract, the Controller obtains information regarding that the earlier identification of the beneficial owner completed during the agency was not appropriate, and consequently, another declaration is required from the customer.

Legal basis of the processing The legal basis of the processing is compliance with the Controller's legal obligation [Article 6(1)(c) of the GDPR]. The processing is provided for in Sections 8-9 of the Anti-Money Laundering Act, and the same Act sets out the conditions of the processing.

The declaration regarding the beneficial owner is based on a legal obligation. If the customer fails to make a declaration regarding the beneficial owner, the Controller will not conclude an agency contract with the customer, or may terminate the contract.

Cases where identification of the beneficial owner is mandatory Pursuant to Section 73(1) of the Anti-Money Laundering Act, the identification of the beneficial owner is mandatory in the case of the following attorney activities:

- management of deposited funds and assets,
- transfer of ownership (share) in a company or other business organisation,
- transfer of ownership of real property,
- foundation, operation and termination of a company or other business organisation,
- unilateral declaration regarding the conclusion of trusteeship contract or trusteeship,
- transfer of movable assets (in particular, funds and financial instruments) for no consideration.

Scope of the data processed The processing covers the following personal data:

- name of the person making the declaration,
- name (name at birth) of the beneficial owner,
- citizenship of the beneficial owner,
- place and date of birth of the beneficial owner,
- home address (or address of residence) of the beneficial owner,
- signature of the person making the declaration.

Term of the processing The Controller shall retain the data for 8 years from the date of fulfilment of the agency, or in the case of a long-term agency, from the date of termination of the business relationship.



In the event of an inquiry from the authority, the Controller shall retain the data for 10 years from the date of fulfilment of the agency, or in the case of a long-term agency, from the date of termination of the business relationship.

Possible recipients of the processing

In the course of the processing, primarily (but not exclusively) the Controller may transmit personal data to the following recipients:

- if the Controller becomes aware of any fact, data or circumstance suggesting money laundering, the Controller will make a report to the Budapest Bar Association,
- the Anti-Money Laundering Information Unit of the National Tax and Customs Administration may submit inquiries to the Controller in the scope of the performance of its tasks.

5. Declaration on qualifying as a politically exposed person

Purpose of the processing

If an agency contract is concluded between the customer and the Controller, then prior to the conclusion of the contract, the customer must make a declaration regarding whether the customer or the beneficial owner qualifies as a politically exposed person, in order to promote the security of legal transactions and to reduce the chance of fraud, money laundering and other criminal offences.

This includes the event where during the term of the agency contract, the Controller obtains information regarding that information suggesting that the customer is a politically exposed person, and consequently, another declaration is required from the customer.

Legal basis of the processing

The legal basis of the processing is compliance with the Controller's legal obligation [Article 6(1)(c) of the GDPR]. The processing is provided for in Sections 8-9 and 16-19 of the Anti-Money Laundering Act, and the same Act sets out the conditions of the processing.

The declaration regarding qualifying as a politically exposed person is based on a legal obligation. If the customer fails to make a declaration regarding whether the customer and/or the beneficial owner is a politically exposed person, the Controller will not conclude an agency contract with the customer, or may terminate the contract.

Scope of the data processed

The processing covers the following personal data:

- name of the person making the declaration,
- the declaration regarding that the customer or the natural person or the beneficial owner of the legal person represented by the customer qualifies as a politically exposed person,
- the reason of qualifying as a politically exposed person,
- name and date of birth of the politically exposed person,



- for a close relative of a politically exposed person, the nature of the relationship,
- the information relating to the source of the funds,
- signature of the person making the declaration.

Term of the processing

The Controller shall retain the data for 8 years from the date of fulfilment of the agency, or in the case of a long-term agency, from the date of termination of the business relationship.

In the event of an inquiry from the authority, the Controller shall retain the data for 10 years from the date of fulfilment of the agency, or in the case of a long-term agency, from the date of termination of the business relationship.

Possible recipients of the processing

In the course of the processing, primarily (but not exclusively) the Controller may transmit personal data to the following recipients:

- if the Controller becomes aware of any fact, data or circumstance suggesting money laundering, the Controller will make a report to the Budapest Bar Association,
- the Anti-Money Laundering Information Unit of the National Tax and Customs Administration may submit inquiries to the Controller in the scope of the performance of its tasks.

6. Records kept regarding the customer identification

Purpose of the processing

In cases where legal representation is mandatory, the Controller keeps records of the identified natural persons. The purpose of the records is to facilitate the security of legal transactions, enforce the limits of the activity of attorneys, and reduce the chance of fraud, money laundering and other criminal offences.

Legal basis of the processing

The legal basis of the processing is compliance with the Controller's legal obligation [Article 6(1)(c) of the GDPR]. The processing is required pursuant to Section 33 of the Attorneys Act, and the same provision provides for the conditions of the processing.

Scope of the data processed

The processing covers the following personal data:

- name (abbreviated name),
- citizenship,
- place and date of birth,
- mother's name,
- home address (or address of residence),
- type and number of identification document,
- a copy of the identification document,
- signature.



Term of the processing The Controller shall retain the data for 8 years from the date of fulfilment of the agency, or in the case of a long-term agency, from the date of termination of the business relationship.

In the event of an inquiry from the authority, the Controller shall retain the data for 10 years from the date of fulfilment of the agency, or in the case of a long-term agency, from the date of termination of the business relationship.

7. Registry of cases

Purpose of the processing Checking compliance with the rules governing the activity of attorneys and providing appropriately protecting the rights of customers.

Scope of the data processed The processing covers the following personal data:

- the case ID created by the Controller,
- the name and address of the customer,
- the subject-matter of the case,
- the date of conclusion of the agency contract,
- the registry number of the judicial proceedings and the reference number of any other proceedings related to the case.

Legal basis of the processing The legal basis of the processing is compliance with the Controller’s legal obligation [Article 6(1)(c) of the GDPR]. The processing is required pursuant to Section 53 of the Attorneys Act, and the same provision provides for the conditions of the processing.

Term of the processing The Controller will process the data and – in the case of countersigning an instrument – the countersigned instrument and the other documents generated in the case associated with the countersigning of the instrument in the registry of cases for the following term:

- 5 years after termination of the agency,
- in the case of countersigning of an instrument, 10 years after the date of countersigning,
- in a case concerning the recording of a right relating to a registry into the public registry, 10 years after the date of recording.

8. Processing related to invoicing

Purpose of the processing The performance of a contract qualifies as an economic event, in the case of which, pursuant to the provisions of Act C of 2000 on Accounting (hereinafter referred to as: “Accounting Act”), the Controller is obliged to retain the accounting records supporting such economic event. The purpose of the processing is the Controller’s compliance with its accounting



obligations, and ensuring that credible evidence is available for certifying the foregoing.

Scope of the data processed

In the course of the processing related to invoicing, the Controller retains the data subject's name, the invoicing address provided by him or her, the number of the agency contract and the designation of the activity conducted.

Legal basis of the processing

The legal basis of the processing is compliance with the Controller's legal obligation [Article 6(1)(c) of the GDPR]. The legal obligation is based on Section 169 of the Accounting Act.

Term of the processing

The Controller will retain the personal data for 8 years after the closing of the financial year.

9. Legal representation in litigation or legal dispute

Purpose of the processing

Exercising or effectuating the rights, legitimate interests or legal claims of the customer in litigation or other, non-litigious legal disputes, and for this purpose, utilising personal data for preparing submissions and documents, and sending to third parties (e.g. another legal person or the court).

Scope of the data processed

The processing typically covers the customer and other data subjects' (for example, the other party in the dispute, witnesses, and other participants of the proceeding) natural personal identification data, home address, and the data necessary for the purpose of the litigation or for establishing or enforcing the legal claim (e.g. personal data in contracts and declarations).

Source of the personal data

The Controller typically receives the personal data from the customer or obtains them from a third party (e.g. via data provision from the company registry, the land registry or the vehicle registry). These data consist mainly of personal data necessary to certify and evidence facts and circumstances.

Legal basis of the processing

If the legislation makes the transmission or utilisation of certain personal data mandatory (e.g. the mandatory substantive elements of the application), the legal basis of the processing is ensuring compliance with the Controller's legal obligation [Article 6(1)(c) of the GDPR]. This includes the case where the court orders the collection of evidence *ex officio*, and the personal data are transmitted for the purpose of complying with the order of the court.

If the legislation does not make it mandatory to transmit or utilise the personal data, but the data are necessary for establishing or enforcing the legal claim, the legal basis of the processing is the legitimate interest of the Controller [Article 6(1)(f) of the GDPR]. The Controller has a legitimate interest in handling the case conscientiously and to the best of his or her



professional knowledge, for which - in most cases - the use of the necessary personal data is indispensable

Term of the processing

The term of the processing is 10 years from the date of termination of the agency contract.

10. Legal representation in administrative proceedings

Purpose of the processing

Representation of the customer in a proceedings conducted before an authority in accordance with the agency contract (e.g. representation of the customer in the proceeding for registration of a trademark or an administrative proceeding initiated against the customer).

Scope of the data processed

The processing typically covers the data subject's (the customer, or for example the customer's employee/customer) natural personal identification data, home address, and the data necessary for conducting the proceeding, managing the case or responding in the administrative proceeding (e.g. the personal data indicated on the form used by the authority or personal data in contracts and declarations).

Source of the personal data

The Controller typically receives the personal data from the customer or obtains them from a third party (e.g. via data provision from the company registry, the land registry or the vehicle registry). These data consist mainly of personal data necessary for certifying and evidencing facts and circumstances.

Legal basis of the processing

Typically, with regard to administrative proceedings, the legislation sets out what personal data are required for initiating the proceeding or during the proceeding. The legal basis of the processing is compliance with a legal obligation [Article 6(1)(c) of the GDPR]. This also includes the case where the transmission of personal data is necessary for example for fulfilling a request or instruction of the authority.

If the legislation does not specify the scope of the personal data processed, but the data are necessary for establishing or enforcing the legal claim, the legal basis of the processing is the legitimate interest of the Controller [Article 6(1)(f) of the GDPR]. The Controller has a legitimate interest in handling the case conscientiously and to the best of his or her professional knowledge, for which - in most cases - the use of the necessary personal data is indispensable.

Term of the processing

The term of the processing is 10 years from the date of termination of the agency contract.



11. Data processing regarding the drafting and countersigning of instruments

<i>Purpose of the processing</i>	Preparation of the instrument requested by the customer (e.g. contract, lawyer's deposit, declaration, will), and utilisation of the personal data in the course thereof. In the case of countersigning an instrument, the purpose of the processing is the preparation of an instrument with full evidencing power.
<i>Scope of the data processed</i>	The processing typically covers the data subjects' natural personal identification data, home address, and the data necessary for preparing the instrument.
<i>Source of the personal data</i>	The Controller typically receives the personal data from the customer or obtains them from a third party (e.g. via data provision from the company registry, the land registry or the vehicle registry). The Controller uses the majority of these data for certifying certain circumstances or for ensuring that the instrument has the legal effect intended to be achieved by the customer.
<i>Legal basis of the processing</i>	<p>If the legislation relating to the instrument sets out the mandatory personal data required for the instrument, the legal basis of the processing is compliance with the Controller's legal obligation [Article 6(1)(c) of the GDPR].</p> <p>If the legislation does not specify the scope of the personal data required for the instrument, but the data are necessary for establishing or enforcing a legal claim, the legal basis of the processing is the legitimate interest of the Controller [Article 6(1)(f) of the GDPR]. The Controller has a legitimate interest in handling the case conscientiously and to the best of his or her professional knowledge, for which - in most cases - the use of the necessary personal data is indispensable.</p> <p>If the subject-matter of the agency is the drafting of an instrument with regard to which the natural person customer only provides his or her own personal data, and the legislation does not specify the scope of the personal data required for the instrument, the legal basis of the processing is the customer's consent [Article 6(1)(a) of the GDPR].</p>
<i>Term of the processing</i>	The term of the processing is 10 years from the date of termination of the agency contract.

12. Processing of data related to legal advice, and preparation of legal opinions

<i>Purpose of the processing</i>	Preparation of legal advice, or a legal opinion for which the use of personal data is required in the case presented by the customer.
----------------------------------	---



<i>Scope of the data processed</i>	The processing typically covers the data subjects' natural personal identification data, home address, and the data necessary for preparing the instrument.
<i>Source of the personal data</i>	The Controller typically receives the personal data from the customer, or obtains them from a third party (for example, by data provision from the business register, land register or vehicle register).
<i>Legal basis of the processing</i>	<p>The processing is mainly necessary for defending or enforcing the customer's legal claim, and therefore the legal basis of the processing is the legitimate interest of the Controller [Article 6(1)(f) of the GDPR]. The Controller has a legitimate interest in handling the case conscientiously and to the best of his or her professional knowledge, for which - in most cases - the use of the necessary personal data is indispensable.</p> <p>If the subject-matter of the agency is the preparation of a legal opinion or position statement with regard to which the natural person customer only provides his or her own personal data, the legal basis of the processing is the customer's consent [Article 6(1)(a) of the GDPR].</p>
<i>Term of the processing</i>	The term of the processing is 10 years from the date of termination of the agency contract.

13. Processing related to applications to job postings and intern positions

<i>Purpose of the processing</i>	The purpose of the processing is to make it possible to contact the applicant via the contact details indicated in the CV or provided by the applicant in order to arrange a job interview or hearing. The Controller will also use the CV for assessing the eligibility of the applicant.
<i>Scope of the data processed</i>	The Controller will process the personal data indicated in the CV or provided by the applicant, such as the applicant's name, home address, email address, and data relating to education and job history.
<i>Legal basis of the processing</i>	The legal basis of the processing is the applicant's consent [Article 6(1)(a) of the GDPR]. The applicant may withdraw his or her consent at any time.
<i>Term of the processing</i>	The term of the processing is typically a few weeks, until the Controller decides who to fill the vacancy or internship position with. If there is more than one applicant to a vacancy or intern position, the Controller will ask for the applicant's consent for retaining the CV for a longer period. If the applicant does not consent to the processing, the Controller will delete the applicant's personal data.



14. Processing related to photos, videos and posts published on the website, social networking sites

<i>Purpose of the processing</i>	In articles, writings and videos published on its website or on social networking sites (in particular LinkedIn, Facebook, YouTube), the Controller shall report on events and activities organised by or with the participation of the Controller, as well as news concerning the law firm.
<i>Scope of the data processed</i>	The processing typically involves the name of the data subjects, their likeness (a photograph and/or video of them) or the personal data they provide (for example in an interview).
<i>Legal basis of the processing</i>	<p>The legal basis of the processing is the legitimate interest of the Controller [Article 6(1)(f) GDPR]. The Controller has a legitimate interest in promoting its activities and raising its profile by reporting, through photographs, videos or posts on its website or social networking pages, on events and activities organised by it or with its participation, as well as news concerning the law firm.</p> <p>The legitimate interest of the Controller is based on the general experience that the attention of readers and users is more attracted by articles, posts with photos or videos.</p>
<i>Term of the processing</i>	As a general rule, the Controller shall ensure the disclosure of personal data until the law firm ceases to exist without successor.

15. Processing related to event registration

<i>Purpose of the processing</i>	Registration of the data subject's intention to participate in an event organised by the Controller.
<i>Scope of the data processed</i>	The data processing covers the name and e-mail address of the data subject and the event for which he or she has registered.
<i>Legal basis of the processing</i>	The legal basis of processing is the data subject's consent [Article 6(1)(a) GDPR]. The data subject may withdraw his or her consent.
<i>Term of the processing</i>	The Controller will delete the personal data within 2 months after the event linked to the registration.



16. Processing of the data of the contact persons of business partners

<i>Purpose of the processing</i>	The purpose of the processing is the establishment of business relations and the performance of contracts concluded with the business partners.
<i>Scope of the data processed</i>	The Controller will process the name, email address and phone number of the designated contact person of the business partner.
<i>Legal basis of the processing</i>	<p>The legal basis for processing is the legitimate interest of the Controller [Article 6(1)(f) of the GDPR].</p> <p>The Controller has a legitimate interest in ensuring that, in order to enter into a contract or other relationship or to perform a contract, an employee of the Controller is able to contact the legal person through the contact person of the legal person.</p>
<i>Term of the processing</i>	The term of the processing is 5 years after the termination of the contract (or contractual relationship) between the Controller and the business partner.

17. Involvement of a processor

SBGK Irodai Szolgáltató és Kereskedelmi Kft. (registered office: H-1062 Budapest, Andrásy út 113.) cooperates as processor in all processing activities. SBGK Kft. is responsible for operating and maintaining the IT system and provides administrative services, in the course of which it has access to personal data to the extent necessary for the performance of its tasks.

18. Fundamental data security measures

The Controller uses several data security measures in order to ensure the security of the personal data, including the following:

- the Controller only uses licensed software and anti-malware programmes, and regularly installs the updates issued by the manufacturer of these software,
- the Controller uses appropriate network security systems,
- the Controller placed the servers in a separate room with restricted access,
- the Controller's employees (attorneys, trainee lawyers, other employees) may access the computer and the mailing system using a unique password specific to them.
- the Controller's employees have a separate drive, which only they can access, and of which backups are made on a regular basis,

19. Rights of the data subject, rules of the exercise of rights

<i>Right to request information</i>	The data subject may request information regarding the processing of their personal data. In this case, the Controller informs the data subject regarding which of the customer's personal data it is processing and for what purpose,
-------------------------------------	--



the legal basis of the processing, the term of the processing, the processor(s), the customer's rights in relation to the processing and the right to file a complaint with the Hungarian National Authority for Data Protection and the Freedom of Information (hereinafter referred to as "the Authority").

Right to request a copy

The data subject may request a copy of the personal data processed by the Controller. In this case, the Controller will send the copy of the personal data to the contact address specified by the data subject (email or postal address).

Right to correction

Upon the data subject's request, the Controller will amend or clarify the data subject's personal data or store the new personal data provided by the customer, if the data subject indicates in his or her request which of his or her personal data is inaccurate and which is the correct personal data.

Withdrawal of consent

If the processing was based on the data subject's consent, the data subject may withdraw his or her consent at any time. The withdrawal of the consent will not affect the lawfulness of the processing conducted prior to the withdrawal.

Right to deletion

The data subject may request the erasure of his or her personal data if

- the personal data are no longer necessary for the purposes for which they were collected;
- the data subject withdraws his or her consent;
- the data subject objects to the processing and the Controller has no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- the personal data must be erased because of a legal obligation to which the Controller is subject.

Right to be forgotten

If the Controller disclosed the customer's personal data and is required to delete the personal data, the Controller will use all reasonable efforts to inform the controllers who received the disclosed data regarding that the customer requested the deletion of the personal data from the Controller.

Right to restriction

- The data subject may request the blocking of personal data if the data subject contests the accuracy of the personal data, for as long as the Controller verifies the accuracy of the data;
- the processing is unlawful, but the data subject opposes the erasure of the personal data and requests instead the restriction of their use;
- the Controller no longer needs the personal data but the data subject requests the blocking of the data for the establishment, exercise or defence of legal claims;
- where the data subject objects to the processing, for the period of time during which the Controller is examining the objection.



Right to data portability The data subject has the right to obtain his or her personal data in a widely-used format (including in particular as a .pdf or .doc file) and to transfer them to another controller. The data subject may request that the Controller transmit his or her personal data to another controller specified by him or her directly.

Right to object The data subject has the right to object against the processing of his or her personal data on the legal basis of interest balancing [Article 6(1)(f) of the GDPR] for reasons related to his or her own situation. In this case, the Controller will assess the arguments made by the customer, and in general, may only continue to process the personal data if the processing is related to the establishment, enforcement or defence of legal claims.

The Controller will fulfil the request within a month, which deadline may be extended by at maximum two months.

In the event of refusal of the request, the Controller will inform the data subject within one month after the receipt of the request regarding the reasons of refusal, as well as the fact that you may place a complaint with the Authority and exercise your right to judicial remedy.

If the Controller has a justified doubt regarding the identity of the person submitting the request, the Controller reserves the right to request submission of the information necessary for confirming the identity of the data subject. Such cases include in particular where the data subject exercises his or her right to the provision of a copy, in which case, it is justified for the Controller to confirm whether the request was made by the person entitled to it.

20. The data subject's avenues of exercising rights

Investigation of the data subject's notification by the Controller. The Controller asks data subjects to notify the Controller of their complaint if they consider that the processing does not comply with data protection requirements before lodging a complaint with the Authority or initiating legal proceedings. The Controller undertakes to investigate the data subject's complaint promptly and to take the necessary corrective measures where justified. The Controller shall inform the data subject of its position and, if the allegation was justified, of the action taken.

The right of recourse to the Hungarian National Authority for Data Protection and Freedom of Information. The data subject has the right to initiate proceedings before the Authority. The Authority's official website (www.naih.hu) contains information on how the data subject can lodge a complaint with the Authority.

Right to apply to the courts. If the data subject considers that the controller has infringed his or her right to the protection of personal data, he or she may also initiate court proceedings and claim compensation for the damage caused to the data subject by the unlawful processing of his or her data or by a breach of data security, and in the case of damage to personality rights, damages. In the event of legal action, the data subject may also bring the action before the courts of the place where he or she resides or is domiciled.