

PRIVACY POLICY OF LAW OFFICE

1. INTRODUCTION

1.1 The following information is provided to our Clients and other persons (hereinafter referred to as "Data Subjects") concerned with the processing of their personal data by Naszádos & Prónay Law Firm (hereinafter referred to as "the Firm" or "the Data Controller"):

1.2. THE IDENTITY OF THE CONTROLLER:

Name: Naszádos and Prónay Law Office

E-mail: titkarsag@nkkb.hu

Telephone: +36 1 269 37 67

Address: 1026 Budapest, Küküllő u. 8.

Sub-office: 1051 Budapest, Szent István tér 11. building A. 602-603. / -

Bar registration number: 635

Tax number: 18097962-2-41

1.3. This Privacy Notice applies only to the personal data of natural persons Data Subjects, with the understanding that the data of legal persons or other entities are not considered personal data.

1.4 In the case of law firms, the following legislation contains important provisions on data processing:

- Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation; also known as GDPR).

- Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (hereinafter referred to as the "Infotv.").

- Act LXXVIII of 2017 on the Activities of Lawyers (hereinafter: Lawyers Act)

- Act LIII of 2017 on the Prevention and Suppression of Money Laundering and Terrorist Financing (hereinafter: Money Laundering Act)

1.5. The Firm does not transfer personal data to a Member State outside the EEA, except where the nature of the assignment requires such transfer. In such cases, the transfer will be subject to appropriate safeguards.

1.6 In many cases, the processing of data by the Agency is based on legislation. In such cases, the data subject is obliged to provide his/her personal data. For example, the conclusion of a mandate contract is subject to the provision of certain personal data by the client and their retention by the lawyer, as defined in the Law on Lawyers and the Money Laundering Act (see point 2.1.6 below). In other cases, the provision of personal data is voluntary, but is in any case necessary for the performance of the mandate. If the data subject fails to provide the personal data that the Firm considers necessary for the performance of the mandate, the Firm may not be able to perform the mandate and thus not be able to provide legal advice to the data subject.

1.7 If the processing is based on consent, the data subject has the right to withdraw his/her consent at any time. However, this does not affect the lawfulness of the processing prior to the consent being given.

2. THE CHARACTERISTICS OF EACH PROCESSING OPERATION

2.1. PROCESSING CARRIED OUT IN THE COURSE OF THE ACTIVITIES OF LAWYERS AND LEGAL ADVISERS

2.1.1. DATA SUBJECTS:

- Natural person clients to whom the Firm provides legal advice or other legal services;
- other natural persons concerned in relation to the mandate given to the Firm (e.g. a party opposing the client in a litigation or dispute, natural persons included in the file of a public authority or litigation, persons heard as witnesses;
- natural person contacts of the Firm's clients.

2.1.2. The Firm also processes certain personal data for the purposes of maintaining contacts, internal case records, invoicing and the enforcement of claims arising in the course of the mandate.

2.1.3. Legal basis:

- The performance of a contract of mandate of a lawyer between the Firm and the data subject (e.g. the performance of a mandate for the preparation and countersigning of a contract for the sale of real estate);
- performance of a legal obligation to which the Firm is subject (see the legal provisions referred to in point 2.1.6 below);
- the legitimate interest of the Firm (e.g. in cases not covered by the legal obligation to keep documents, to keep them for the purpose of subsequent proof of performance, to maintain contact during the performance of the mandate, to ensure the integrity of the file management, to recover claims). Legitimate interests: uniform registration and management of files, the right to claim a fee for the mandate and to ensure unhindered communication during the performance of the service;
- legitimate interest of a third party (e.g. the legitimate interest of the person instructing the Office to enforce a claim of the instructing party, in relation to the processing by the Office of personal data of the debtor of the claim, or, for example, in relation to the processing of personal data of a litigant against the Office's instructing party in a legal proceeding, or of witnesses heard in a legal proceeding or of persons included in the case file). Legitimate interests of third parties: interest in the enforcement of claims and the settlement of disputes.

2.1.4. For specific cases defined by law, see point 2.1.6 below.

2.1.5 Recipients: the Firm will only transfer personal data to third parties if this is necessary for the performance of the assignment. In the case of legal deposits, for example, the law requires the reporting of the deposits to the Budapest Bar Association or, in certain cases, the Money Laundering Act requires the reporting of the deposits. For the legal requirements, see point 2.1.6 below.

2.1.6. THE STATUTORY DATA PROCESSING FOR THE ACTIVITIES OF LAWYERS, THE SCOPE OF THE DATA PROCESSED

2.1.6.1. LAWYERS ACT

2.1.6.1.1. IDENTIFICATION

The lawyer shall identify a natural person whom he does not know or whose identity is in doubt by consulting his identity document.

In order to check the validity of the documents of natural persons and the consistency of the data contained in the register kept by the lawyer, the lawyer is entitled to request electronically the following data from the register of identity and address, the register of driving licences, the register of travel documents and the central register of aliens:

- a) natural person identification data,
- (b) nationality, statelessness, refugee, immigrant, settled or EEA national status,
- c) address,
- (d) facial image,
- (e) signature,
- f) facts pursuant to Article 18(5) of Act LXVI of 1992 on the Registration of Personal Data and Address of Citizens,
- g) data pursuant to Article 24(1)(f) of Act XII of 1998 on Travel Abroad and the period of validity of the document,
- h) the data pursuant to Article 8(1)(b)(ba)-(b)(b) of Act LXXXIV of 1999 on Road Traffic Registration,
- i) the data pursuant to Section 76(d), Section 80(1)(b) and (c) of Act I of 2007 on the Entry and Residence of Persons with the Right of Free Movement and Residence and Section 95(1)(g), Section 96(1)(g) and Section 100(1)(b) and (c) of Act II of 2007 on the Entry and Residence of Third-Country Nationals.

If the natural person's client is represented by a proxy, the lawyer may dispense with the separate identification of the client if the power of attorney containing the client's particulars

- has been countersigned by a lawyer,
- by a notary,
- the signature of the agent is notarised,
- or the power of attorney has been authenticated or re-authenticated by the Hungarian diplomatic mission or consular post competent for the place of signature or has been certified by an Apostille certificate.

If the lawyer represents the natural person in proceedings for registration in a public register or draws up a document on the basis of which the legal representative is registered in a public register, the natural person's data must be consulted in the register.

2.1.6.1.1.2. RECORD OF TRANSACTIONS REQUIRING MANDATORY LEGAL REPRESENTATION

The lawyer must keep a register of transactions requiring mandatory legal representation. The register of identified natural persons shall contain the following information:

- natural person identification data,
- address,
- nationality, statelessness, refugee, immigrant, settled or EEA national status,
- type and number of the identification document used for identification,
- the identifier of the response received when requesting data from the register,
- the case identifier of the cases where identification of the natural person is mandatory,
- data specified in the Act on the Prevention and Combating of Money Laundering and Terrorist Financing.

The register of identified legal persons and other entities contains the following personal data:

- natural person identification data of the person acting on behalf of the identified legal person or other entity,
- data specified in the Law on the Prevention and Combating of Money Laundering and Terrorist Financing.

The lawyer shall keep changes to the data in the register in such a way that the previous data remain available.

The data in the above register shall be kept by the Firm for the period specified in the Money Laundering Act (8 years).

2.1.6.1.1.3. CONVERSION OF A PAPER DOCUMENT INTO AN ELECTRONIC DOCUMENT

The lawyer may convert a paper document into an electronic document in certain cases specified by law. In such cases, the lawyer must keep the electronic document for 10 years and the paper document for 5 years, unless the parties agree on a longer period.

2.1.6.1.1.4. PROCESSING OF LEGAL DEPOSITS

The lawyer shall record the details of the deposits in excess of twice the amount of the statutory minimum wage which he administers and any changes thereto in an electronic deposit register maintained by the regional bar association.

The electronic deposit register shall record:

- the name and the Bar identification number of the depositing lawyer,
- the case identifier of the deposit contract,
- the type of deposit,
- the subject of the deposit,
- if the depository lawyer places the deposit in a sub-account, the sub-account number,
- in the case of a cash deposit, the amount of money actually deposited and the currency denomination,
- the date of the conclusion, amendment or termination of the escrow agreement,
- the date of recording of the data in the deposit account register and the date of any modification of the recorded data.

The data and any changes thereto shall be recorded by the lawyer within one working day of the conclusion of the escrow agreement or change of data by means of a qualified electronic signature and a time-stamped electronic declaration. The electronic register shall assign a unique identification number to the deposit.

The electronic deposit record shall contain the data for 10 years after the termination of the deposit contract.

2.1.6.1.1.5. CASE AND DOCUMENT MANAGEMENT

A lawyer shall keep a record of the matters handled under the mandate in order to ensure that compliance with the rules governing the practice of the profession of lawyer can be verified and to protect the rights of clients in the event of the termination of the right to practise as a lawyer.

The register of cases shall contain the following information:

- the case identifier provided by the lawyer,
- the name of the client,
- the subject matter of the case,
- the date of the contract of engagement, and
- the registration number of the court proceedings relating to the case and the file number of other proceedings.

The lawyer shall keep the data for 5 years after the termination of the mandate, 10 years after the countersignature of the deed in the case of countersignature of a deed, and 10 years after the registration of the deed in the case of registration of a right to immovable property in the Public Registry.

The register may be consulted and requested only by the staff or body carrying out the official control of the Bar and, in order to protect the rights of the client, by the deputy lawyer and the designated registrar.

The lawyer shall keep the deed he has countersigned and other documents relating to the matter for which the deed was countersigned for a period of 10 years from the date of countersignature, unless a longer period is provided for by law or the parties have agreed to keep them for a longer period.

In the event of the termination or cessation of his membership of the Bar or his removal from the Bar register, the lawyer shall ensure that the documents which he has handled and which cannot be discarded are handed over to the client or to the lawyer who is practising the profession of lawyer in the case in question and who is entitled to handle the document, and that the records are kept in accordance with the Lawyers Act.

2.1.6.2. THE MONEY LAUNDERING ACT.

2.1.6.2.2.1. CUSTOMER DUE DILIGENCE

The Money Laundering Act requires lawyers to provide client due diligence in the following cases:

- if he/she is a custodian of money and valuables
- if he/she acts as a lawyer under the Lawyers Act in connection with the preparation and execution of the following transactions:
 - o the transfer of ownership of a share (participation) in a business company or other economic entity,
 - o transfer of ownership of real estate,
 - o the establishment, operation or dissolution of a company or other business entity;
 - o a trust deed or unilateral declaration of trust
 - o the transfer without consideration of movable property, in particular of funds or financial assets.

Measures involving proof of the identity of the client

- In the case of natural persons, the Agency is obliged to record the natural person:
 - surname and first name,
 - name and surname at birth,
 - nationality,
 - place and date of birth,
 - mother's name at birth,
 - address or, in the absence of such address, place of residence,
 - type and number of his/her identification document;

- In the case of a legal person or an unincorporated organisation, the Agency is obliged to record the following personal data (the other data to be recorded in this case are those of the organisations):

- o the names and titles of the persons authorised to represent the entity,
- o the names and titles of the persons who are to act as agents of the agency.
- o the identity of the agent.

The lawyer must require the production of the following documents in order to verify the identity of the person concerned:

- For natural persons:

- In the case of a Hungarian citizen, his/her official identity card and official proof of address,
- In the case of a foreign national, his/her travel document or identity card, provided that it entitles him/her to reside in Hungary, his/her document certifying the right of residence or his/her document entitling him/her to reside in Hungary,
- In the case of a legal person or an organisation without legal personality, the person authorised to act on its behalf or on its behalf:

- in the case of a Hungarian citizen, his/her official identity card and official certificate of residence,
- in the case of a foreign national, his/her travel document or identity card, provided that it entitles him/her to reside in Hungary, his/her document certifying the right of residence or his/her document entitling him/her to reside in Hungary.

The lawyer must make copies of the documents and certificates presented.

- Rules on proof of beneficial ownership

The natural person client must make a written declaration by personal appearance, in a manner determined by the supervisory authority, by means of a pre-audited electronic communication medium, that he is acting in the name or on behalf of the beneficial owner.

- What information must the lawyer include in this declaration about the beneficial owner?

- o surname and forename
- o surname and forename at birth
- o nationality
- o place and date of birth
- o address or, in the absence thereof, place of residence

- The lawyer must also ask the client for information on whether the beneficial owner is a prominent public figure

The representative of the client of a legal person or an unincorporated entity must make a written declaration in person, by means of a pre-audited electronic communication medium, in a manner determined by the supervisory authority, that he or she is acting on behalf of or in the interest of the beneficial owner.

- What information must the lawyer include in this declaration about the beneficial owner?

- o surname and forename
- o surname and forename at birth
- o nationality
- o place and date of birth
- o address or, in the absence thereof, place of residence
- o the nature and extent of the ownership interest

- The lawyer must also ask the client for information on whether the beneficial owner is a prominent public figure

In which cases can the beneficial owner's certificate be waived? If, on the basis of a risk-sensitive approach, the lawyer records the information on the basis of documents presented to the lawyer or records available to the lawyer confirm it. (However, in such cases, the lawyer must also record the fact of the omission.)

2.1.6.2.2. MEASURES RELATING TO BUSINESS RELATIONSHIP AND TRANSACTION DATA

The lawyer must record the following information on the business relationship and the transaction:

- in the case of a business relationship, the type, subject and duration of the contract,
- in the case of a transaction, the subject matter and amount of the engagement,
- the circumstances of performance (place, time, manner).

The lawyer may, on the basis of a risk-sensitive approach, request information on the source of funds and the production of documents relating to the source of funds in order to verify this information.

The lawyer must ensure that the information and documents available on the client and the business relationship are up to date.

The lawyer must check the validity and accuracy of the information at least every 5 years. If in doubt as to whether the information is up to date, the lawyer shall repeat the client due diligence measures.

When is the lawyer obliged to carry out a check to verify the identity of the client and the beneficial owner?

As a general rule, you must carry out identity verification of the customer and beneficial owner before establishing a business relationship or executing a transaction, and may exceptionally carry out it during the establishment of a business relationship if this is necessary to avoid disruption to the normal course of business and if the likelihood of money laundering or terrorist financing is low. In this case, the verification of identity shall be completed before the first transaction is concluded.

Customer due diligence measures need not be repeated if

1. the lawyer has already carried out the client due diligence measures in relation to the client, the authorised representative, the authorised agent and the representative in connection with another business relationship or transaction,
2. the identity of the client, agent, nominee or representative has been established in connection with the present business relationship or transaction, and
3. no changes have been made to the data.

Purpose limitation, record keeping, statistics

Personal data obtained in the course of the customer due diligence, other than the customer's lawyer, may be accessed and processed by the customer solely for the purposes of the performance of its tasks in the prevention and combating of money laundering and terrorist financing, and to the extent necessary for the performance of those tasks:

- the head of the lawyer
- a member of his/her assisting family
- employee

How long do we have to keep the data processed under the Money Laundering Act? We are obliged to keep the data required by law for 8 years from the date of termination of the business relationship or from the date of completion of the transaction (this applies to personal data, data that does not constitute personal data, documents and copies thereof).

The lawyer is also obliged to record in the register transaction orders executed in cash (in HUF or in foreign currency) for an amount of HUF 3 million to 600,000 or more, which information he is obliged to keep for 8 years.

At the request of a supervisory body, the financial information unit, the investigative authority, the public prosecutor's office and the court, the information must be kept for the period specified in the request, but not longer than 10 years from the termination of the business relationship or the execution of the transaction order.

An extension on the basis of a request is only possible if the data or documents specified therein are necessary for the purposes of ongoing or future proceedings. After this period has expired, it must delete or destroy it without delay.

2.2. CONTACTING, COMPLAINT HANDLING, REQUESTING A QUOTE

2.2.1. Data subjects: natural persons contacting the Office, requesting a quotation, enquiring or lodging a complaint, as well as natural persons who are contact persons of such undertakings.

2.2.2.2 Purpose of processing: in case of contact by the Data Subject, the purpose of processing depending on the purpose of the contact (e.g. replying to enquiries received by filling in a contact form, preparing a quotation, replying to incoming e-mails, dealing with the substance of a complaint and informing about the action taken, etc.)

2.2.3. The data processed: name (filling in the contact form on the Agency's website is mandatory), e-mail address (filling in the contact form on the Agency's website is mandatory), telephone number, address (depending on the data communicated by the Data Subject or the channel of communication), name and position of the company, if applicable, and other data provided in the request.

2.2.4 Legal basis for processing. Legitimate interest: ex-post verifiability of the information contained in the communication with the customer, complaint handling, quality assurance.

2.2.5 Duration of processing: depending on the nature of the communication or complaint, but in any case for at least 5 years after the complaint has been settled

2.3. CCTV surveillance

2.3.1 Data subjects: persons entering the premises of the Office.

2.3.2. Protection of the cash flow in the headquarters, premises and branches of the Firm, as well as the protection of products, equipment, technical goods and other valuables of significant asset value located there, their value and preservation. The camera system operated for these purposes is a security solution designed to prevent accidents and offences involving damage, to detect infringements and to provide evidence of such infringements in the context of official or judicial proceedings.

2.3.3. Scope of data processed: image and facial image, observed behaviour

2.3.4. The consent is informed by means of signs on the premises.

2.3.5 Duration of data processing: 3 days after the recording is made in the absence of use

2.3.6. Recipients: in the event of infringement or criminal proceedings, the authorities or courts conducting the proceedings

2.4. STAFF SELECTION

2.4.1 Data subjects: persons applying for a job or selected in connection with a specific job advertisement.

2.4.2 Purpose of processing. Where the specific purpose of the collection of personal data is different, it will be explicitly indicated in the line below. The purposes of processing after the assessment of the application are: (i) to keep the files necessary to prove the position of the controller in the event of a claim by the applicant (legal basis for the latter processing: legitimate interest, see the information on this in the section "Legal basis for processing"), (ii) and, if the applicant specifically consents, to direct contacts by the controller with a view to making further job offers.

2.4.3. SCOPE OF DATA PROCESSED:

- Name, date and place of birth, nationality, permanent address, place of residence (purpose of processing: identification of the applicant)

- Telephone number, e-mail address (purpose of processing: contact)

- Details of the position applied for

- Data concerning educational qualifications

- Data relating to professional experience

- Data on language skills

- Skills, competences

- Where relevant: curriculum vitae and details of the CV, e.g.

- o Portrait, if included in the CV

- o Natural identity data (name, gender, date and place of birth, nationality)

- o language skills, educational and other qualifications, professional experience, preferred position, field of interest

- o type of driving licence, if applicable, and any other information given in the CV.

- Where relevant: covering letter and its contents.

2.4.4. LEGAL BASIS FOR PROCESSING:

- Consent of the applicant. Please note that you are not obliged to give your consent. However, if you do not consent to the processing of your data for recruitment purposes, we will not be able to assess your application. If you have given your consent, you may withdraw it at any time without giving any reason, but such withdrawal will not affect the lawfulness of the processing that took place before the withdrawal.

- The legal basis for the processing of data after the assessment of the application is the legitimate interest of the controller (legitimate interest being the preservation of evidence necessary in the event of a possible claim by the applicant, the possibility of subsequent proof of the lawfulness of the controller's actions), unless the applicant has given his/her consent to further requests.

2.4.5. THE DURATION OF THE PROCESSING:

- In the case of an unsuccessful application, 12 months after the date of the decision on the job application.

- If the applicant has given specific consent, the data will be kept and used by the controller for a further 2 years in order to contact the applicant to consider further job offers.

- In the event of a successful application, the controller will continue to process the data provided at the time of application only to the extent necessary to establish and maintain the employment relationship, in accordance with the specific information to be provided to employees.

2.5. TRAINEESHIP PROGRAMME

2.5.1.

2.5.2 Purpose of data processing: to provide internship opportunities, to identify the intern, to assign the intern appropriate tasks, to maintain contact, to issue an internship certificate.

2.5.3. SCOPE OF DATA PROCESSED:

- Name, date and place of birth, nationality, permanent address, place of residence (purpose of processing: identification of the applicant)

- Telephone number, e-mail address (purpose of data processing: contact)

- Data concerning language skills (in the case of candidates for an intellectual job)

- Skills, abilities

- If necessary: CV and the data contained therein, e.g.

o portrait, if included in the CV

o natural identity data (name, sex, date and place of birth, nationality)

o language skills, educational and other qualifications, professional experience, preferred position, field of interest

o type of driving licence, if applicable, and any other information given in the CV.

- Where relevant: covering letter and its contents.

2.5.4 Legal basis for processing: consent of the Data Subject

2.5.5 Duration of processing: 5 years from the end of the traineeship, unless the Data Subject's data (e.g. name) are contained in a data medium which the Agency is obliged to keep for a longer period.

3. PROCESSING OF DATA

3.1 A data processor is a natural or legal person or any other body which processes personal data on behalf of the controller. The data processor may not take any substantive decision concerning the processing, may process personal data coming to his knowledge only in accordance with the provisions of the Agency, may not process personal data for his own purposes and shall store and keep the personal data in accordance with the provisions of the Agency.

3.2. These persons are considered as data processors for the purposes of processing personal data. You can obtain information on the specific identity of the data processors by contacting the Office.

4. DATA SECURITY

4.1 The Agency shall ensure the security of data in accordance with the relevant regulations. In particular, the Office shall take the technical and organisational measures and establish the procedures to ensure that the data processed are protected

against unauthorised access, alteration, disclosure, transmission, publication, deletion, destruction, accidental destruction or accidental damage and against inaccessibility resulting from changes in the technology used.

4.2 When defining and applying measures to ensure the security of data, the Office shall take into account the state of the art. The Agency will choose the one of several possible data processing solutions which ensures a higher level of protection of personal data, unless this would impose a disproportionate burden on the Agency. The Office shall also apply these requirements vis-à-vis its processors.

4.3 The data controller shall provide different levels of access rights within the software used, according to the user hierarchy. In order to avoid loss of data, the contents of computers and servers shall be backed up. In the premises of the controller, only administrators are authorised to access the server rooms. IT systems are protected by appropriate firewalls. The controller shall ensure that the IT system is adequately protected against viruses. The controller shall provide appropriate training to its employees on data security requirements. The controller shall maintain strict standards for the activities of the data processors it uses.

4.4 The Agency undertakes to require all third parties to whom it may transmit or transfer data to comply with the above undertakings. However, in the event of lawful transmission of data by the Agency, the Agency shall not be liable for any damage caused by the recipient.

4.5.

5.

5.1 The Data Subject may, at any time, request information on the processing of personal data concerning him or her, request the rectification, erasure or restriction of the processing of personal data concerning him or her, and object to the processing of such personal data, using the contact details indicated in this notice. The Data Subject also has the right to data portability.

5.2. Where necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further two months. The Office shall inform the data subject of the extension of the time limit, stating the reasons for the delay, within one month of receipt of the request. If the request has been made by electronic means, the information shall also be provided by electronic means, if possible, unless the data subject requests otherwise. If we consider that we do not need to take action on the Data Subject's request, we will inform the Data Subject without delay, but at the latest within one month of receipt of the request, of the reasons for non-action and of the possibility to lodge a complaint with the DPA and to exercise his or her right to judicial remedy.

5.3.

5.4 If there are reasonable doubts as to the identity of the Data Subject submitting the request, he/she may be asked to provide additional information necessary to confirm his/her identity.

5.5. At the request of the Data Subject, the Agency shall provide information on whether or not his/her personal data are being processed and, if so, the Data Subject shall have the right to obtain access to the personal data concerning him/her processed by the Agency, as well as information on the purposes of the processing, the categories of data concerned, the recipients or categories of recipients to whom the personal data have been or will be disclosed, the envisaged duration of the processing or the criteria for determining the duration, and the source of the data.

5.6. Upon request, the Agency shall provide the Data Subject with a copy of the personal data subject to processing. Additional copies requested by the Data Subject may be charged a reasonable fee based on the administrative costs. If the Data Subject has submitted the request by electronic means, the information shall be provided in a commonly used electronic format, unless otherwise requested by the Data Subject. If the natural person of the Data Subject has not been identified beforehand and the lawyer/staff member of the Law Firm handling the case does not know the Data Subject personally, the provision of personal data pursuant to this point shall be subject to the identification pursuant to Article 32(2) of Act LXXVIII of 2017, subject to the provisions of point 5.4.

5.7 The Data Subject may request the rectification of inaccurate data and has the right to request the completion of incomplete data.

5.8 The Data Subject may request the Agency to delete personal data if

1. they are no longer necessary for the purposes for which they were processed;
2. if the Data Subject withdraws his/her consent and there is no other legal basis for the processing;
3. the Data Subject has objected to the processing and the conditions set out in point 5.13 apply;
4. the processing is unlawful;

5. they must be erased in order to comply with a legal obligation to which the Agency is subject,
6. the Data Subject is a minor under the age of 16.

5.9.

1. the exercise of the right to freedom of expression and information,
2. to comply with a legal obligation to which the Agency is subject,
3. the establishment, exercise or defence of legal claims

or for the protection of the interests of the Office.

5.10. At the request of the Data Subject, the Agency restricts the processing of personal data if

- a) the Data Subject contests the accuracy of the personal data, in which case the restriction shall apply for the period of time necessary to allow the accuracy of the data to be verified,
- b) although the processing is unlawful, the Data Subject opposes the erasure and requests the restriction instead,
- c) the Office no longer needs to process the data but the Data Subject requests the processing for the establishment, exercise or defence of legal claims,

(d) the Data Subject has objected to the processing in accordance with point 5.13, in which case the restriction shall apply for a period of time until it is determined whether the legitimate grounds of the Controller prevail over the legitimate grounds of the Data Subject.

5.11. Where processing is subject to restriction on the basis of the above, such personal data, with the exception of storage, may only be processed with the consent of the Data Subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another person or for important public interests of the Union or of a Member State. The Office shall inform the Data Subject who requests the lifting of the restriction in advance.

5.12. The Agency shall notify the Data Subject of the rectification, erasure or restriction, as well as all those to whom the data were previously communicated. The Agency will not notify the data subject if this is impossible or requires a great effort. If the Agency has disclosed the personal data and is obliged to delete them, it will take reasonable steps, including technical measures, taking into account the available technology and the cost of implementation, to inform the other controllers that process the data that the Data Subject has requested them to delete the links to the personal data in question or a copy or duplicate of such personal data.

5.13. The Data Subject may object to the processing of his or her personal data,

1. a) if it is based on legitimate interest; in this case, the processing may not proceed, unless it is justified by compelling legitimate grounds which override the interests, rights and freedoms of the Data Subject or by reasons relating to the establishment, exercise or defence of legal claims,
2. b) if it is for the purposes of or in connection with direct marketing; in such a case, processing for these purposes may no longer be carried out.

5.14. On the basis of the right of data portability, the Data Subject may, on the one hand, request the Office to provide him/her with his/her personal data processed in a structured, commonly used, machine-readable format, where technically feasible, and to transmit it to any data controller, and, on the other hand, request the Office to transmit his/her data.

5.15. If the Agency does not comply with the Data Subject's request as referred to above, it shall inform him/her of the reasons for the non-fulfilment within one month of receipt of the request at the latest.

5.16. If the Data Subject considers that his/her rights in relation to his/her personal data have been infringed, he/she is requested to notify the Agency of his/her complaint using one of the contact details provided.

5.17. If you decide to do so, you can report it to the authority using the contact details below:

National Authority for Data Protection and Freedom of Information.

Address.

Address for correspondence: 1363 Budapest, PO Box 9.

Phone: +36-1-391-1400

Fax: +36-1-391-1410

E-mail: ugyfelszolgalat@naih.hu

5.18. If you are aware of unlawful processing, you may also bring a civil action. The court has jurisdiction to hear the case. You can also bring a lawsuit before the court in your place of residence (for a list of courts and their contact details, please see the following link: <http://birosag.hu/torvenyszekek>).

6. The Privacy Notice in force at the time of registration of the Data Subject or when he/she otherwise provided his/her personal data, even if a previous Privacy Notice was in force, will always apply to the processing of personal data.

7. CONTACT

7.1 If you have any questions, comments or requests regarding this privacy notice, or if you wish to make a complaint or exercise any of the rights detailed above, please contact us using the contact details below:

Name: Naszádos and Prónay Law Office

E-mail: titkarsag@nkkb.hu

Telephone: +36 1 269 37 67

Address: 1026 Budapest, Küküllő u. 8.