PRIVACY POLICY

Data Controller

Name	**Daniel Palotai dr. Law Firm** **Daniel Palotai dr. attorney-at-law**
Registered seat	H-1145 Budapest, Amerikai út 90/F.
Record number of the Budapest Bar Association	36066727
Phone	+36 30 9918 402, +36 1 332 0075
E-mail	iroda@palotaidaniel.hu

The Data Controller is responsible for the design, enforcement and implementation of any necessary changes of the present Privacy Policy. The effective version of this Privacy Policy is always available on the Data Controller's website.

1. Purpose of the Privacy Policy

Daniel Palotai dr. attorney-at-law (hereinafter: "Data Controller") is committed to the protection and security of personal data and respects the right to informational self-determination of the data subjects. Therefore, preparing this Privacy Policy, the Data Controller has taken into account the principles, requirements and provisions related to the processing of personal data without exception and it takes all necessary technical and organizational measures to ensure the security of personal data. For this reason, the Data Controller provides in this Policy transparent and comprehensible information on how it processes the personal data of identified or identifiable natural persons (hereinafter "Data Subjects") during their visit to the website www.palotaidaniel.hu.hu (hereinafter "Website") and in the course of providing services related to the activities of the Data Controller, taking into account the legal requirements and principles governing lawful and appropriate data processing, data protection and the safeguarding of the right to informational self-determination.

This Privacy sets out the purposes of the processing of personal data processed by the Controller in the course of and in relation to the provision of its services, the legal basis, the duration of the processing, the recipients, i.e. who has access to the Data Subjects' personal data, and the rights of the Data Subjects in relation to the processing of their personal data. The Data Controller shall process the Personal Data of Data Subjects only for the purposes set out in this Policy and to the extent necessary for the fulfilment of those purposes, in accordance with lawful processing, the principles and requirements of data protection and security and the Data Subjects' right to informational self-determination.

The Data Controller invites the Data Subjects to read this Policy carefully and to follow any future changes to it.

2. Scope and application of the present Policy

The present Policy sets out the processing of personal data of website visitors, clients and contractual partners of the Data Controller (hereinafter referred to as "visitors, clients or data subjects").

3. References to acts of law

The Policy is primarily based on the following acts of law:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46 (General Data Protection Regulation) (hereinafter: **GDPR**),
- Act CXII. of 2011 on the Right to Information Self-Determination and Freedom of Information (hereinafter: Information Act),
- Act. CVIII of 2001 Act on Certain Issues of Electronic Commerce Services and Information Society Services (hereinafter: E-Commerce Act),
- Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing (hereinafter: Anti-Money Laundering Act),
- Act LXXVIII of 2017 on the professional activities of Lawyers (hereinafter: Lawyers Act),
- Act XXV of 2023 on complaints, disclosures in public interest, and related rules on reporting abuses (hereinafter: Whistleblower Protection Act),
- Act V of 2013 on the Civil Code (hereinafter: Civil Code),
- Act CL of 2017 on the Rules of Taxation (hereinafter: Taxation Act),
- Act C of 2000 on Accounting (hereinafter: Accounting Act).

4. Definitions

data processor: any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

data management or data processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

restriction of data management: marking of stored personal data in order to limit their future processing.

data controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by the European Union or Member State law.

erasure: making data unrecognisable so that it is no longer possible to recover.

recipient: the natural or legal person, public authority, agency or any other body, whether or not a third party, to whom or with whom the personal data are disclosed or shared.

data subject: The identified or identifiable natural person to whom the personal data that is processed is related.

data subject's consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

personal data: any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

5. Data subjects concerned by the processing

The Data Controller processes the data of the following data subjects in the course of providing the services available on the Website:

- Visitors,
- Clients,
- potential clients, i.e. natural persons who contact the Data Controller in order to use the services available on the Website,
- authorised representatives of a legal person,
- where applicable, other persons involved in the provision of the service.

6. Scope of the data processed by the Data Controller

The Data Controller defines the main categories of the processed data as follows:

- the data necessary to identify the Data Subjects
  - first and last name;
- contact data
  - e-mail address, residence, address, telephone number;
- data necessary for the preparation of a contract, for the provision of services, for the conclusion of a contract, for the enforcement of rights and obligations of the contract or for the settlement after the termination of a contract
  - the data required for identification and contact purposes as described above, as well as the type and subject of the contract;
- documents containing the data necessary for the Data Controller to fulfil its legal obligation to provide data about the Data Subject
  - accounting documents, data of payment transactions, personal data necessary for the fulfilment of the attorney's legal obligation to carry out the client's identification according to the provisions of the Lawyers Act and the Anti-Money Laundering Act;
- data required by law for the handling of complaints and reports according tot he Whistleblower Protection Act
  - name, contact data, address, telephone number, depending on the form of the complaint or report.

7. Purposes of data processing

The Data Controller shall process only personal data that is necessary for the purpose of the processing or for achieving the result of the processing.

The Data Controller defines the possible purposes of the processing of personal data as follows:

- the identification of the Data Subjects,
- communication,
- preparation and conclusion of contracts,
- enforcement of contractual rights and obligations,
- settlement after the termination of a contract,
- legal obligation of the Data Controller to provide data about the data subject,
- the legitimate interests of the Data Controller as set out in this Policy;
- complaint and report handling.

8. Legal basis for data processing

The Controller processes the personal data of Data Subjects on the following legal basis or bases:

- the Data Subject has given his or her explicit consent to the processing of his or her personal data for one or more specific purposes,
- the processing is necessary for the performance of a contract to which the Data Subject is a party, or for taking steps at the request of the Data Subject prior to entering into the contract,
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- the 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;
- the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The Data Controller shall ensure that one of the above legal bases is maintained for the entire duration of the processing. If a legal basis no longer exists, for example because the Data Subject has withdrawn his or her consent and there is no other legal basis for processing the data, the ongoing processing of the data is unlawful and the Data Controller shall delete the data from all its records, including paper records or electronic storage.

The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

9. Duration of storage

Data retention period

The Data Controller stores each category of data as follows:

- personal data for a period of 5 years from the termination of the contract related the use of the Data Controller's services (termination of the attorney’s agreement), otherwise 5 years from the final and binding decision in the case subject to the attorney’s agreement,

- contracts of sale and purchase, documents of company proceedings for 10 years from the date of the contracts or the documents pursuant to the Lawyers Act,

- transaction data, accounting documents pursuant to paragraph 169 section (2) of the Accounting Act, and personal data related to the fulfillment of legal obligations under the Anti-Money Laundering Act for a period of 8 years,

- data collected and processed during the communication until the purpose of the processing is fulfilled,

- the data processed in the course of a complaint, the documentation of the complaint for the period necessary for the processing and handling of the complaint, at the latest 5 years from the date of the complaint in order to enable the Data Controller to prove that it acted in compliance with the law in the event of any legal dispute,

- data processed on the basis of consent until the consent is withdrawn.

10. Method of data storage

The storage of personal data is subject to the principles of lawful and purposeful processing. The Data Controller stores personal data in identifiable form in accordance with its internal policies, which set out general rules and procedures for the retention of personal data.

The Data Controller shall take appropriate technical and organisational measures to keep personal data confidential and secure. Personal data shall be stored by the Data Controller in its own IT systems or those of its Service Providers and Partners, which are certified having adequate level of security, preventing unauthorised access, in locked and separate premises pursuant to the Lawyers Act.

11. Data processing activities

11.1. Contacting the Data Controller

Data processed: name, contact data and other data provided by visitors, clients or potential clients and the designated contact personnel of potential business partners

Purpose of data processing: answering visitors', potential clients' and business partners' questions, handling potential clients's requests

Legal basis for processing: pursuant to Article 6 section (1) a) of the GDPR, the data subject gives his or her consent to the processing by contacting the Data Controller, sending a message and providing his or her contact data. The name and contact data of the designated contact personnel of business partners are processed by the Data Controller on the basis of the legitimate interest of the parties pursuant to Article 6 section (1) f) of the GDPR, as it is in the

legitimate interest of the parties to maintain the communication for business purposes. The data subject has the right to object to the processing concerning his or her data.

Duration of processing: until the purpose of the processing is fulfilled or the data subject's consent is withdrawn. The data subject may withdraw his or her consent at any time by sending a written statement to the Data Controller's address. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Data of the designated contact person of the business partner shall be processed by the Data Controller until the data subject objects to the processing.

Data transfer, access to data: The Data Controller may transfer the data to DotRoll Kft. (H-1148 Budapest, Fogarasi út 3-5.) for web-hosting purposes.

11.2. Provision of services, execution of mandates, legal practice

Data processed: Client's or Partner's first and last name, e-mail address, billing details, address, telephone number, personal data recorded in the contract/attorney's agreement, data processed during the execution of the mandate (e.g. case number, date, subject of the agreement/mandate), identification numbers and photocopies of personal documents

Purpose of data processing: fulfilling the mandate, acting as a legal representative, providing information and negotiating the details of the mandate, issuing invoices, accounting and tax obligations, client identification obligations

Legal basis for data processing:

- preparation and/or performance of a contract of which the data subject is one of the parties pursuant to Article 6 section (1) b) of the GDPR;
- pursuant to Article 6 section (1) c of the GDPR to comply with the legal obligation of the controller pursuant to paragraph 169 section (2) of the Accounting Act, paragraph 32 section (1), (3) of the Lawyers Act and paragraph 6 of the Anti-Money Laundering Act

Duration of data processing: purchase data are processed until the end of the 8th year after the invoice was issued, pursuant to paragraph 169 section (2) of the Accounting Act, and

until the end of the 8th year from the date of issue of the invoice pursuant to paragraph 169 section (2) of the Accounting Act, until the end of the 8th year from the date of client identification pursuant to paragraph 56 section (2) of the Anti-Money Laundering Act, and according to paragraph 53 section (3) of the Lawyers Act until 5 years after the termination of the mandate, in the case of countersigning a deed until 10 years after the date of the countersigning of the deed, and in the case of registration of a right to real property in a public register until 10 years after the registration of the right in the public register. Data will be processed beyond this period only for the purpose of the fulfilment of a legal obligation, if applicable.

Data transfer:

- the transfer of payment data for the purpose of processing the payment,
- the Customer's name, telephone number and delivery address will be transferred to the courier service in order to fulfil the order.

Data transfer, access to data: invoice data will be transferred to KBOSS.hu Kft. (számlázz.hu, H-1031 Budapest, Záhony u. 7.), and the Data Controller may transfer the data to DotRoll Kft. (H-1148 Budapest, Fogarasi út 3-5.) for web-hosting purposes.

Mandatory provision of data: the provision of the data necessary for the fulfilment of the contract (mandate) and invoicing is mandatory, as the Data Controller is unable to fulfil the contract and his legal obligations without the data.

11.3. Complaints and whistle blowing system

Data processed: name, contact data, other data provided in the complaint/report

Purpose of data processing: handling complaints/reports, enforcement of clients' rights, fulfilling legal obligations

Legal basis for data processing: with regard to article 6 section (1) c) GDPR, the fulfilment of the legal obligation of the Data Controller pursuant to paragraph 18 section (2) of the Whistleblower Protection Act

Duration of processing: since the Data Controller has joined the whistleblowing system operated by the Hungarian Bar Association, the Data Controller does not keep the complaints/reports received directly by the Data Controller, but informs the complainant that he or she can file a report with the Hungarian Bar Association

Data transfer, access to data: invoice data will be transferred to KBOSS.hu Kft. (számlázz.hu, H-1031 Budapest, Záhony u. 7.), and the Data Controller may transfer the data to DotRoll Kft. (H-1148 Budapest, Fogarasi út 3-5.) for web-hosting purposes

11.4. Invoices

Data processed: name, address, tax number (if applicable), invoice data

Purpose of data processing: verification of the transaction, fulfilment of accounting obligations

Legal basis for data processing: the fulfilment of a legal obligation pursuant to Article 6 section (1) c) of the GDPR based on paragraph 169 section (2) of the Accounting Act

Duration of data processing: until the end of the 8th year after the invoice was issued

Data transfer, access to data: invoice data will be transferred to KBOSS.hu Kft. (számlázz.hu, H-1031 Budapest, Záhony u. 7.), and the Data Controller may transfer the data to DotRoll Kft. (H-1148 Budapest, Fogarasi út 3-5.) for web-hosting purposes

Mandatory provision of data: with regard to the statutory accounting obligations of the Data Controller, the provision of the data is mandatory as the Data Controller is not able to issue an invoice without the data.

12. Cookies

A cookie is a small data file saved on your computer to help you store settings and other information about the pages you visit, and to identify the device you are using.

Cookies are placed on the visitor's browser by the server of the visited site or other service provider, which saves them on the device used by the visitor. Each time a page is loaded, the visitor's browser sends the cookie again to the server, which reads it and uses it for a specific purpose. Only cookies necessary for the operation of the website may be placed on the visitor's device without the visitor's consent (session cookies and cookies for the purposes of fraud prevention, etc.). These cookies may be deleted or blocked, but in this case it is not certain that the website will function properly.

The placement of other third-party cookies, such as social media cookies for statistical or marketing purposes requires the visitor's consent and authorisation. The visitor can set, modify or delete cookies in his/her browser.

The Data Controller uses Google Analytics-solutions for monitoring the services and analysing the users' activities. The placement of cookies of Google Analytics assists in transferring the users' needs to the servers and in measuring statistical recordings of the website of the services, in monitoring the user' activities and in determining where the user uses the services. Therefore, the Data Controller uses the cookies of third parties for measuring and analysing the above performance of the users, including the services of Google Analytics. Unsubscribing from this may be carried out on the websites of the third parties' services, by the Google Analytics Opt-out Browser. Cookies placed for these purposes may only be installed upon the user's consent thereto. In the scope of Google Analytics, the technical data transferred by the web browser of the user shall not be combined with other Google data (https://policies.google.com/privacy?hl=en-US). By appropriate configuration of the user's browser, you may prevent these cookies from being stored.

Cookies from third parties used on this website:

Source (website, domain name)	Cookie name	Cookie function, type (required cookie/other purpose cookie)	Cookie duration
Google Analytics	_ga	Statistics	2 years
Google Analytics	_gid	Statistisc	24 hours

13. Data security

The Data Controller undertakes to ensure the security of the data, to take technical and organisational measures and to establish procedural rules to ensure that the data recorded, stored or processed are protected and to prevent their destruction, unauthorised use or unauthorised modification. The Data Controller shall take all necessary measures to ensure the secure processing of data and the establishment and operation of the necessary procedures and internal systems. The Data Controller shall ensure that the processed data cannot be accessed, disclosed, transmitted, modified or deleted by unauthorised people.

The Data Controller shall, taking into account the state of science and technology and the cost of implementation, as well as the nature, scope, context and purposes of the processing and the varying likelihood and severity of the risk to the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of data security appropriate to the level of risk, where applicable:

- the pseudonymisation and encryption of personal data;
- the confidentiality, integrity, availability of the systems and services used to process personal data;
- in the event of a physical or technical incident, the ability to restore access to personal data,
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing,
- in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Some examples of the security measures applied by the Data Controller:

- access to the data recording and storage servers of the Data Controller and of the Service Providers that process data for the Data Controller is restricted to employees who are responsible for the processing of personal data,
- the information technology systems, networks and servers of the Data Controller and those of its Service Providers are protected by anti-virus, firewall and other protection softwares,
- the Data Controller shall establish effective internal procedures to prevent and respond to data breaches, including promptly notifying the Data Subject where necessary,
- the destruction of the data is also carried out in accordance with the data protection provisions and the procedures established by the Data Controller for this purpose.

14. Data transfer, data provision

14.1. Data transfer in the context of data processing

The Data Controller is also entitled to involve third parties in activities involving personal data, including, for example, the storage of data on servers owned by the Service Provider, Partner; IT services and support provided by the Service Provider, Partner, data recording by an external company, use of payment systems, etc. The Data Controller shall only use a data processor that provides adequate guarantees for compliance with the GDPR requirements for data processing and for the additional guarantees required for the implementation of appropriate technical and organisational measures to ensure the protection of the rights of the Data Subjects.

The Data Controller enters into a data processing agreement with the service provider, under which the service provider assists and/or supports the Data Controller in providing services and fulfilling its contractual obligations. In the context of a processing operation carried out by a processor acting on behalf of or under the instructions of the Controller, the processor shall act in accordance with the instructions of the Data Controller. Data processing agreements shall comply in form and content with the applicable requirements of the GDPR and the model data protection agreements and contractual provisions approved by the National Authority for Data Protection and Freedom of Information (NAIH) in its recommendations.

The Data Controller's processors:

- IT services provided by a data processor,
- Data recording, other administrative activities, accounting activities carried out by a data processor,
- Services provided by a data processor in connection with invoices.

14.2. Contractual data processors

The Data Controller currently uses the services of the following data processors:

- Web hosting service: DotRoll Kft. (H-1148 Budapest, Fogarasi út 3-5.)
- Accounting service: Activum Tax Kft. (H-1173 Budapest, Szürkebegy utca 93-97. 2. a., accountant: Ákos Peőcz)
- Invoicing: K-BOSS.hu Kft. (számlázz.hu, H-1031 Budapest, Záhony u. 7.)

15. Enforcement of the data subjects' rights

Pursuant to the provisions of Articles 15-20 GDPR, the data subject has the following rights:

- Right of access
- Right to rectification
- Right to erasure (‘right to be forgotten’)
- Right to restriction of processing
- Right to object to the processing

- Right to data portability
- Right to withdraw his or her consent at any time.

The data subject may send a request to exercise these rights to any of the contact addresses of the Data Controller. The Data Controller shall provide information on the action taken on the request without undue delay and at the latest within 30 days after the receipt of the request. If the Data Controller fails to take action, it shall inform the Data Subject without undue delay and at the latest within 30 days after the receipt of the request of the reasons of its failure. The Data Controller shall inform each recipient to whom or with whom the personal data have been disclosed or shared of any rectification, erasure or restriction of processing, unless this is impossible or involves a disproportionate effort.

If the Data Controller does not provide a satisfactory response to the data subject's request, the data subject shall have the right to judicial legal remedies.

16. The rights of Data Subjects

16.1 Right of access by the data subject

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source.

16.2 Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

16.3 Right to erasure

The Data Subject may request the erasure of his or her data if:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- the processing is unlawful,
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the erasure is ordered by a court or the NAIH.

16.4. Right to restriction of processing

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

16.5 Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

16.6 Right to data portability
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 without hindrance from the controller to which the personal data have been provided, where the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and the processing is carried out by automated means.

16.7 Right to withdraw consent
Where the Data Subject has given his or her consent to the processing of his or her personal data, he or she may withdraw it at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Where the data are necessary in another context with a proper legal basis (e.g. archiving obligations under law), the data may only be used for that purpose and their availability shall be limited for all other uses.

16.8. Complaint
The Data Subject may file a complaint at any time if he or she has suffered a real or perceived breach of rights in relation to his or her personal data. The Data Controller will take all reasonable steps to ensure that the processing of the data subject's request is carried out in a manner that is fair to the data subject.

17. Legal remedies
The Data Subject

- may file a complaint with the National Authority for Data Protection and Freedom of Information (represented by Dr. Attila András Péterfalvi, registered seat: Falk Miksa u. 9-11., 1055 Budapest; address: H-1363 Budapest, Pf. 9; telephone: +36-1-391-1400; fax: +36-1-391-1410; e-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu);
- may file a claim with the court in the place of his or her residence in order to initiate court proceedings.