

PRIVACY POLICY

TABLE OF CONTENT

1. PURPOSE OF THE PRIVACY POLICY	3
2. DATA OF THE CONTROLLER.....	4
3. DATA PROCESSING CONCERNING CONTACTING AND COMMUNICATION	5
3.1.1. PROCESSED PERSONAL DATA AND PURPOSE OF PROCESSING.....	5
3.1.2. LEGAL BASIS OF PROCESSING.....	5
3.1.3. DURATION OF THE PROCESSING	5
3.1.4. MODE OF PROCESSING	6
3.1.5. DATA PROTECTION CONTRACTUAL CLAUSE.....	6
3.2. PROCESSING OUR CLIENT'S DATA.....	7
3.2.1. THE PERSONAL DATA PROCESSED	7
3.2.2. THE LEGAL BASIS OF PROCESSING.....	8
3.2.3. THE DURATION OF PROCESSING	8
3.2.4. THE WAY OF THE STORING PERSONAL DATA	9
3.2.5. THE PROVIDING OF THE PERSONAL DATA.....	9
3.3. PROCESSING OF DATA OF THIRD PARTIES RELATED TO OUR CLIENTS.....	10
3.3.1. THE PERSONAL DATA PROCESSED AND THE PURPOSES OF THE PROCESSING	10
3.3.2. THE LEGAL BASIS OF DATA PROCESSING	10
3.3.3. THE DURATION OF DATA PROCESSING.....	10
3.3.4. THE WAY OF THE STORING PERSONAL DATA	10
3.4. PROCESSING CONCERNING INVOICING.....	11
3.4.1. PROCESSED PERSONAL DATA AND PURPOSE OF PROCESSING.....	11
3.4.2. LEGAL BASIS OF PROCESSING.....	11
3.4.3. DURATION OF THE PROCESSING	11
3.4.4. MODE OF PROCESSING	11
3.4.5. PROVISION OF PROCESSING.....	11
4. WHAT ARE YOUR RIGHTS?	12
4.1. RIGHT TO ACCESS	12
4.2. RIGHT TO RECTIFICATION	12
4.3. RIGHT TO ERASURE.....	12
4.4. RIGHT TO BE FORGOTTEN.....	13
4.5. RIGHT TO RESTRICTION OF PROCESSING.....	13
4.6. RIGHT TO DATA PORTABILITY	14
4.7. RIGHT TO OBJECT.....	14
4.8. RIGHT TO LODGE COMPLAINT	14

5. MEASURES AND NOTIFICATION	15
5.1. INFORMING DATA SUBJECTS	15
5.2. MODE AND DEADLINE OF NOTIFICATION.....	15
5.3. MONITORING	15
5.4. COSTS OF MEASURES AND NOTIFICATIONS.....	15
6. POSSIBLE RECIPIENTS	16
6.1. DURING THE OPERATION OF OUR WEBSITE.....	16
6.2. SOCIAL MEDIA	16
6.3 FACEBOOK.....	16
7. COOKIES	18
7.1. COOKIES IN GENERAL	18
7.2. OUR COOKIES	18
7.3. COOKIE SETTINGS	19
8. DATA SECURITY	20
8.1. ORGANIZATIONAL MEASURES.....	20
8.2. TECHNICAL MEASURES	20
9. OTHER PROVISIONS	21
9.1. PROCESSING FOR DIFFERENT PURPOSE.....	21
9.2. DATA PROTECTION	21
9.3. RECORD OF PROCESSING.....	21
9.4. DATA BREACHES.....	21
9.5. CHANGES TO OUR PRIVACY POLICY	21
APPENDIXES	22
APPENDIX 9.1 THE RELEVANT LEGAL ACTS	22
APPENDIX 9.2 DEFINITIONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA	23
APPENDIX 9.3 THE DATA SUBJECT’S RIGHTS	25

1. Purpose of the Privacy Policy

The goal of our Privacy Policy is to provide all necessary information about processing your personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and assist the Data subjects in exercising their rights under Section 4.

The legal basis of our duty to communicate information is Article 12 of Regulation 2016/679 of the European Parliament and Council (hereinafter referred to as: GDPR) and the relevant Hungarian data protection regulations.

In the Privacy Policy, we may define you as “data subject”, or “contact person of our business partners” in the following.

You may find further definitions concerning your personal data within the Appendix of the current Privacy Policy.

2. Data of the controller

Name	dr. Dobos István Attorney at Law
Registry number	19810 (Budapest Bar Association)
Registered seat	1117 Budapest, Völgycsillag utca 4., 6. emelet 02. a.
E-mail	dobos@doboslegal.eu
Telephone number	+3630 3088151

3. Data processing concerning contacting and communication

It is possible to connect us through our availabilities located on the website. Also, by communicating with our business partners, we process the personal data of their contact person. The details of these processing are described hereunder.

3.1.1. Processed personal data and purpose of processing

personal data	purpose of processing
name	identification of the Data subject, or the contact person of our business partner
phone number	contacting and communication with the Data subject, or the contact person of our business partner
e-mail address	contacting and communication with the Data subject, or the contact person of our business partner

3.1.2. Legal basis of processing

If you contact us through our website, we process your personal data on your freely given consent that you provide in the moment of your connection by phone or email (article 6 (1) a) of GDPR).

If you, as the representative of our business partners provide your personal data to communicate with us, the legal basis of processing personal data is the legitimate interest of us and our business partners (section 6 paragraph 1 point f of GDPR). It is each Party's legitimate interest to maintain an effective business communication and to perform the contract. Since it is the part of your scope of duty (representation of our business partners), in our view, processing your name and contact data doesn't restrict disproportionately your privacy and freedom of self-determination.

3.1.3. Duration of the processing

If you contact us through our website, we process your personal data until the withdrawal of your consent. You have the right to withdraw your consent at any time via email. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

In relation to the processing of the personal data of our business partners' contact persons, we process their personal data until the personal data are no longer necessary in relation to the purposes for which they were collected or as long as it is possible according to the relevant acts (pursuant to the Hungarian

Civil Code, 5 years following the performance or the termination of the contract, or 8 years following invoicing, in accordance with the Hungarian accounting act).

3.1.4. Mode of processing

Your personal data are collected manually, in electronic form.

3.1.5. Data protection contractual clause

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing concerning communicating with our business partners, we, as data controllers, while performing the contracts concluded with our business partners, both at the time of the determination of the means for processing, and at the time of the processing itself, implement appropriate technical and organizational measures, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of GDPR.

3.2. Processing our Client's data

On the basis of attorney agreement, when we provide legal services to our Clients, we must comply with the following laws and regulations governing data processing:

- Act LXXVIII of 2017 on the activities of attorneys-at-law (hereinafter referred to as: Act on the activities of attorneys-at-law)
- Act LIII of 2017 on the prevention and prevention of money laundering and terrorist financing (hereinafter referred to as: Act on the prevention and prevention of money laundering and terrorist financing)
- Rule of Hungarian Chamber of Lawyers of 14/2018. (VI. 25.) in Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing and in the Act LII of 2017 implementing the financial and property restrictive measures imposed by the European Union and the United Nations Security Council, on compliance with specific obligations, risk assessment, monitoring procedures and guidance (hereinafter referred to as: Rules of Hungarian Chamber of Lawyers)
- Act C of 2000 on accounting (hereinafter referred to as: Act on accounting)

3.2.1. *The personal data processed*

In relation to Section 32 (1) of Act on the activities of attorneys-at-law, with the exception of the mandate for legal advice, we are obliged to carry out the Client due diligence measures under Section 7 of Act on the prevention and prevention of money laundering and terrorist financing before concluding the mandate contract. We must record the following data, in accordance with the rules of Hungarian Chamber of Lawyers:

a) natural person

- family name and given name,
- family name and given name at birth,
- nationality,
- place and date of birth,
- address, in the absence of this, place of residence,
- mother's maiden name,
- the type and number of the identity document;

b) legal entity or an organisation without legal entity

- the names and functions of the authorised representatives,
- the identity document of the person authorised to effect service.

According to the Rules of Hungarian Chamber of Lawyers, we are required to check and make photocopies of the following identity documents of our Clients (during this process, the picture of our Client on their ID card is also recorded as personal data.);

- in the case of Hungarian citizens, the page of the official card, that proves their identity and address and does not contain their personal identification number,
- in the case of foreign nationals, their travel document or identity card, provided that it entitles them to reside in Hungary, their document certifying their right of residence or their document entitling them to reside in Hungary.

In addition to this personal data, our Clients will necessarily provide other personal data (for example: telephone number, e-mail address for contact), which we process exclusively for the purpose of fulfilling the contract of engagement. Personal data provided by our Clients may include financial, payment, bank account, contact and health information, as well as any other information relevant to the fulfilment of the order.

3.2.2. The legal basis of processing

We process the above personal data of our Clients for the purposes of the performance of the attorney agreement between us (Article 6 (1) b) of GDPR).

We have a legal obligation to record and monitor the personal data of our Clients, and the legal basis for our processing in this regard is as follows the Article 6 (1) c) of GDPR, the Section 32 of Act on the activities of attorneys-at-law, and the Section 7 of Act on the prevention and prevention of money laundering and terrorist financing.

If our Client is a legal entity, the legal basis for the processing of the contact person's personal data (name, email address, telephone number) is the legitimate interest of the processor and the Customer. (Article 6 (1) f) of GDPR). Each party has a legitimate interest in ensuring effective business communication and in ensuring that the other party's designated representative is informed of all material facts relating to the contract between us. Our client's contact person has an employment or contractual obligation to facilitate communication between the parties and to provide personal data for this purpose, so in this case there is no infringement of his or her right to information self-determination.

3.2.3. The duration of processing

We are entitled to process the personal data of our Clients for a period of eight years from the fulfilment of the attorney agreement. (Section 56 (2) of Act on the prevention and prevention of money laundering and terrorist financing).

The organisations defined in Article 5 of Act on the prevention and prevention of money laundering and terrorist financing, at the request of the financial information unit, the investigating authority, the

public prosecutor's office and the court, must retain the data for the period specified in the request, but for a maximum of ten years from the date of the execution of the attorney agreement (Section 58 (1) of Act on the prevention and prevention of money laundering and terrorist financing).

3.2.4. The way of the storing personal data

Both on paper and in electronic format.

3.2.5. The providing of the personal data

In view of the fact, that we are not able to execute the attorney agreement without knowing the personal data contained in this clause, the provision of personal data is a precondition for the conclusion of the contract.

3.3. Processing of data of third parties related to our Clients

In the course of completing attorney agreement, we get to know the employees of our Clients, and the personal data of partners, service providers, parties opposing legal or administrative proceedings and their representatives in relation to our Clients.

3.3.1. The personal data processed and the purposes of the processing

The personal data as defined in point 3.1.1 relating to third parties that we process in the context of an attorney agreement is always processed for the purposes set out in the attorney agreement.

3.3.2. The legal basis of data processing

In the course of legal representation in judicial or administrative proceedings, the data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us. (Article 6 (1) e) of GDPR)

In the case, that we do not process personal data of third parties in the context of judicial or administrative proceedings, the legal basis for the processing is the legitimate interest of us or our Clients. (Article 6 (1) f) of GDPR); to complete the attorney agreement, we need to know the information that our customers give us. For example, when giving an opinion on an employer's notice of termination, we need to know the employee's date of birth to determine the statutory notice period. We process personal data for specified purposes and in relation to the needs of our Clients and applicable laws. In our view, our data management practices do not result in an unjustified restriction of the privacy and informational self-determination of the third parties concerned.

3.3.3. The duration of data processing

In view of the fact that information of attorney agreement is stored in our records according to the category of the Clients, the storage period for personal data of third parties involved in the case is the same as described in section 3.1.3.

3.3.4. The way of the storing personal data

Both on paper and in electronic format.

3.4. Processing concerning invoicing

After the performing of the orders we – with regard to Act C of 2000 on accounting – make out a bill. The details of such processing are described hereunder.

3.4.1. Processed personal data and purpose of processing

personal data	purpose of processing
name	confirmation of the accounting
address	confirmation of the accounting

3.4.2. Legal basis of processing

Processing is necessary for compliance with a legal obligation; with regard to section 6 paragraph 1 point f of GDPR, section 5 article 1 point b of Information Act and section 166 paragraph 1 to 3 of Act C of 2000.

3.4.3. Duration of the processing

8 years after accounting.

3.4.4. Mode of processing

Personal data are collected manually, in electronic form.

3.4.5. Provision of processing

Since we cannot perform our accounting obligations without knowing any information about you, the processing is a statutory requirement.

4. What are your rights?

4.1. Right to access

You have the right to obtain confirmation as to whether or not personal data concerning you are being processed, and, where that is the case, access to the personal data and the information featured in point 3.

You have the right to access to the following information concerning the processing of your personal data:

- 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 organizations;
- 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 us rectification or erasure of personal data or restriction of processing of personal data concerning you or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- the existence of automated decision-making, including profiling, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

4.2. Right to rectification

You have the right to obtain from us without undue delay the rectification of inaccurate personal data concerning you. Taking into account the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

4.3. Right to erasure

You have the right to obtain from us the erasure of personal data concerning you without undue delay and we shall have the obligation to erase personal data without undue delay if it is mandatory according to Article 17 of GDPR. The erasure of your personal data is obligatory for us in the following instances:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- you withdraw consent on which the processing is based, and where there is no other legal ground for the processing;
- you object to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- 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.

4.4. Right to be forgotten

If we made the personal data public and are obliged to erase your personal data, we inform controllers which are processing the personal data that you have requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

We do not make your personal data public.

4.5. Right to restriction of processing

You have the right to obtain from us restriction of processing if is obligatory according to Article 18 of GDPR. Such instances are the following:

- the accuracy of the personal data is contested by you, for a period enabling us to verify the accuracy of the personal data;
- the processing is unlawful and you oppose the erasure of the personal data and requests the restriction of their use instead;
- we no longer need the personal data for the purposes of the processing, but they are required by you for the establishment, exercise or defense of legal claims;

If you obtain restriction of processing in accordance with the above, we inform you before the restriction of processing is lifted.

4.6. Right to data portability

You have the right to receive the personal data concerning you, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from us if it is possible according to Article 20 of GDPR. Where technically feasible, you have the right to have the personal data transmitted directly from us to another controller.

4.7. Right to object

You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on point (f) of Article 6(1) of GDPR (see: point 3.2. of the current policy). In such case, we no longer process the personal data unless we demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defense of legal claims.

4.8. Right to lodge complaint

You have the right to appeal to the Hungarian courts and to make a complaint to the Hungarian (<https://naih.hu/>) Supervisory Authority.

5. Measures and notification

5.1. Informing Data subjects

We communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 of GDPR to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. We also inform you about those recipients on the request of yours.

5.2. Mode and deadline of notification

We provide information on action taken on a request under Articles 15 to 22 of GDPR to you without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We inform you of any such extension within one month of receipt of the request, together with the reasons for the delay. Where you make the request by electronic form means, we provided the information by electronic means where possible, unless you request it otherwise.

If we do not take action on your request, we inform you without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy (see point 4.7.).

5.3. Monitoring

If we have reasonable doubts concerning the identity of the natural person making the request, we may request the provision of additional information necessary to confirm the identity of the data subject.

5.4. Costs of measures and notifications

We provide you information and take the necessary measures free of charge.

If your requests are manifestly unfounded or excessive, in particular because of their repetitive character, we may charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested or we refuse to act on your request.

6. Possible recipients

6.1. During the operation of our website

Our website's hosting provider (data processor) can have access to the personal data you provide while using the website. The data processor's data are the following:

Name: Dotroll Kft.

Connection: <https://dotroll.com/hu>

6.2. Social media

Our website has several social media profile so that if you „like” us on Facebook or „follow” us on Instagram, we may learn all the personal data which is public on your profile.

6.3 Facebook

Meta Platforms Ireland Limited (registered office: 4 Grand Canal Square Grand Canal Harbour Dublin 2, Ireland, Irish company registration number: 462932, website: <https://about.facebook.com/meta>) offers a range of Meta products that include Facebook (including the Facebook mobile app and browser in the app). In connection with the use of Facebook, the Terms of Use and Privacy Policy/Privacy Notice of Meta Platforms Ireland Limited will govern the existing data processing depending on the specific purpose of the processing:

- Together with Meta Platforms Ireland Limited, we are responsible for the processing of the Users' personal data for the purposes of collecting audience, delivering messages, personalising features and content, and improving and securing Meta products. To comply with the GDPR, an agreement on the allocation of responsibilities and information on the Privacy Shield Framework for data transfers are available under the following links:

https://www.facebook.com/legal/Workplace_GDPR_Addendum

https://www.workplace.com/legal/WorkplaceEuropeanDataTransferAddendum?fbclid=IwAR1KngiTZgbBM7CxwiyX7937hOazemFX9svQl34lMfVEwNjkhdbuDUDF_9A

- In the context of joint processing, Meta Platforms Ireland Limited is primarily responsible for providing information about the processing and enabling data subjects to exercise their rights under GDPR. For more information on the processing of Users' personal data by Facebook and the rights and possibilities available to the User in this regard, please see the Meta Platforms Ireland Limited Privacy Notice for Facebook, available under: <https://www.facebook.com/about/privacy/>.

- In other respects, the parties are individually responsible for the processing of personal data.

Our processing is based on the User's consent, in accordance with article 6 section 1) a) of GDPR. The User may withdraw his or her consent at any time for the future by changing his or her preferences set in the cookie field. Withdrawal of consent does not affect the lawfulness of the processing prior to the withdrawal of consent.

7. Cookies

7.1. Cookies in general

In order to the proper functioning of our websites, we have placed smaller data files in computer devices of Users in certain cases, similarly to most of the modern websites.

Cookies are small text files, which the website places to the computer device (including mobile phones) of the user. Consequently, the website is able to “remember” the settings of the user (such as: applied language, letter size, design, etc.), therefore, it is not necessary to set it each time the user visits our website. A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.

Cookies may be either "persistent" cookies or "session" cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.

Cookies do not typically contain any information that personally identifies a user, but personal information that we store about you may be linked to the information stored in and obtained from cookies. Cookies can be used by web servers to identify and track users as they navigate different pages on a website and identify users returning to a website.

The pixel tag is a small tag or graphic element, which is placed on the services, on other websites, in e-mails or other downloadable materials other than the computers, mobile devices or web browsers unless the user downloads the content. The pixel tag does not store information on the computer, mobile device or web browser (although an e-mail or other downloadable material on the computer may contain such), therefore it may not be set, only by deleting the material including such pixel tag.

7.2. Our cookies

The names of the cookies that we use on our website, and the purposes for which they are used, are set out below:

Source of cookie	Name of cookie	Function of cookie	Duration of cookie
Google Inc.	Google reCAPTCHA	protection against SPAM's	persistent

Before sending messages, we perform a reCAPTCHA check using Google's reCAPTCHA service. This feature works through Google servers. The reCAPTCHA function is processed by Google, and we do not process any personal data or receive any information about users or their behaviour. The reCAPTCHA check is necessary to ensure that the form is not filled in by robots designed for this purpose and to prevent mass spam messages from being sent to us. Google's servers automatically perform the authentication process, we do not have access to any personal data. The reCAPTCHA check does not add anything to the content of the message. The data and information provided in messages

sent via the form will only be used to answer the sender's questions and will not be stored in the database. Emails sent in this way do not entitle you to receive newsletters, offers or notifications of downloads, so we do not send such emails to the contact email address in the letter. The cookie(s) may be deleted or blocked, but in this case the functionality of the Website may not work properly. The cookie(s) cannot be used to personally identify the User. These cookie(s) are only for the purposes described above.

7.3. Cookie settings

Cookie files can be deleted (see www.AllAboutCookies.org for details) or blocked from being placed by most browsers today. In this case, however, you will have to re-configure certain settings each time you use our Website and some services may not work.

Detailed information on how to delete or block cookies can be found at www.AllAboutCookies.org and for the browser used by the User under the following links:

- [Firefox](#)
- [Google Chrome](#)
- [Bing](#)

8. Data security

We secure your personal information from unauthorized access, use or disclosure. We secure the personally identifiable information you provide on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure. When personal information (such as connection data) is transmitted to other Web sites, it is protected through the use of encryption, such as the Secure Socket Layer (SSL) or HTTPS protocol.

Our employees and the employees of the data processors have the right to get acquainted with the personal data of the User, to the extent necessary, for the performance of the tasks which belong to their job. We make all technical and organizational measures that guarantee the security of the data.

8.1. Organizational measures

We provide access to our IT systems with personalized rights. The “necessary and sufficient rights” principle applies to the allocation of accesses, consequently all employees may use our IT systems and services only to the extent necessary for the performance of their duties, with the appropriate rights and for the required time. Access to IT systems and services can only be granted to a person who is not restricted for security or other reasons (e.g. conflicts of interest) and who has the professional, business and information security knowledge required to use it securely.

We and the data processors undertake strict confidentiality rules in a written statement, and we are obliged to act in accordance with these confidentiality rules during the course of our activities.

8.2. Technical measures

The data is stored, with the exception of the data stored by our data processors, on our own devices, in a data center. The IT devices which store data are located in an isolated, separate closed server room, protected by a multi-stage access control system subject to authorization control.

We protect our internal network with multi-level firewall protection. In all cases, a hardware firewall (border protection device) is located at the entry points of the applied public networks. The data is stored redundantly, that is, in several places, so it is protected from destruction, loss, damage, or illegal destruction due to the failure of the IT device.

Our internal networks are protected from external attacks with a multi-level, active protection against complex malicious code (e.g. virus protection). The external access to the IT systems and databases is operated by us via an encrypted data connection (VPN).

We do steps to ensure that the IT tools and software continuously comply with the generally accepted technological solutions in the market.

We develop systems, during our development, in which logging can be used to control and monitor the operations performed, and to detect incidents, such as unauthorized access.

Our server is protected and closed, located on the dedicated servers of the hosting provider.

9. Other provisions

9.1. Processing for different purpose

If we intend to further process the personal data for a purpose other than that for which the personal data were collected, we provide the you prior to that further processing with information on that other purpose and with any relevant further information.

9.2. Data protection

We secure your personal information from unauthorized access, use or disclosure. We secure the personally identifiable information you provide on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure. When personal information (such as connection data) is transmitted to other Web sites, it is protected through the use of encryption.

9.3. Record of processing

To comply with section 30 of GDPR, we maintain a record of processing activities under our responsibility.

9.4. Data breaches

Data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. In case of data breach, we act according to section 33 and 34 of GDPR.

9.5. Changes to our Privacy Policy

We will occasionally update this Privacy Policy to reflect feedback. We encourage you to periodically review this Policy to be informed of how we are protecting your information.

Effective: 2023.02.09.

dr. Dobos István Attorney at Law
Controller

Appendixes

Appendix 9.1 The relevant legal acts

In the course of drafting this Privacy Policy, the Controller has taken into account the relevant effective legal acts and the international recommendations, with special regard to the following:

- 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 (GDPR)
- Act CXII of 2011 on the right of informational self-determination and on freedom of information (Information Act);
- Act V of 2013 on the Civil Code (Civil Code);
- Act CXXX of 2016 on the Code of Civil Procedure (Pp.);
- Act CVIII of 2011 on electronic commerce and on information society services (Electronic Commerce Act).

Appendix 9.2 Definitions with regard to the processing of personal data

- ‘controller’ means the legal person, which determines the purposes and means of the processing of personal data;
- ‘processing’ means 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- ‘data transfer’ means making accessible of the data for a third person;
- ‘data erasure’ means making the data unrecognisable in a manner that the recovery of the data is no longer possible;
- ‘marking of data’ means the provision of an identification mark for the data for the purposes of differentiation;
- ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;
- ‘destruction of data’ means the entire physical destruction of the data carrier containing the data;
- ‘processor’ means the legal person, which processes personal data on behalf of the controller;
- ‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
- ‘cookie’ means the small data package (text file) sent by the web server and placed for a definite time on the Data Subject’s computer, which the server, depending on its nature, may complement at the time the website is visited again, that is, if the web browser sends back a previously saved cookie, then the service provider processing such cookie has the possibility to combine the Data Subject’s current visit with the previous one, but only with respect to its own content;
- ‘data subject/Data Subject’ means an identified or identifiable natural person; 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
- ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

- ‘consent’ of the data subject means 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;
- ‘IP-address’ means the IP-address, that is, an identification number of server machines in every network that uses the TCP/IP protocol for communication, which enables the identification of the specific devices through the network. It is well-known that each computer device connected to the network has an IP address, by which it may be identified;
- ‘personal data’ means any information relating to the data subject;
- ‘objection’ means the statement of the data subject, by which he/she objects to the processing of his/her personal data and requests the termination of data processing or the erasure of the processed data.

Appendix 9.3 The Data Subject's rights

Right to access

The Data Subject is entitled to receive access to the personal data being processed by us, at his/her request, submitted to any address as indicated in our contact details. In the scope thereof, the Data Subject may be informed of the following:

- whether his/her personal data are being processed;
- 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,
- where possible, the envisaged period for which the personal data will be stored,
- his/her rights
- the possibility for redress
- information in relation to the source of data

The Data Subject may request a copy of his/her personal data that is subject to the processing of data. In this case we shall provide the personal data in a structured, commonly used and machine-readable format (PDF/XML) and on paper, in a printed format. Requesting the copy is free of charge.

Rectification

Based on a request submitted to any address as indicated in our contact details, the Data Subject is entitled to request the rectification of the inaccurate personal data concerning him/her and to have the incomplete data completed. If we do not have the necessary information for the correction and completion of the incorrect information, we may request the provision of such supplementary data and the certification of the accuracy of the data. In the absence of such supplementary information, we shall restrict the processing of the relevant personal data and we shall temporarily suspend the measures carried out thereon with the exception of storing until such a time that the correction and completion of data may be performed.

Erasure

Based on a request submitted to any address as indicated in our contact details, the Data Subject is entitled to request the erasure of the personal data concerning him/her and processed by us, provided that any of the following conditions are met:

- we no longer need the provided personal data;

- the Data Subject expresses concern with regard to the lawfulness of his/her data being processed by us.

Should we determine based on the Data Subject's request that we are obligated to erase the personal data processed by us, we shall cease the processing of such data and we shall destruct the previously processed personal data. Besides that, we are also obligated to erase the personal data upon the revocation of consent, the exercising of the right to object and based on our obligations laid down in legal acts.

Restriction of data processing

Based on a request submitted to any address as indicated in our contact details, the Data Subject is entitled to request the restriction of the personal data concerning him/her processed by us in the following cases:

- the Data Subject expresses concern with regard to the lawfulness of the data concerning him/her, being processed by us and restriction is requested instead of erasure;
- we no longer need the provided data, but they are required for the establishment, exercising or defending of the Data Subject's claims.

We automatically restrict the processing of personal data if the Data Subject challenges the accuracy of the personal data and the Data Subject exercises his/her/its right of objection. In this case, the restriction shall extend to such a time period which enables the checking of the accuracy of the personal data and, in case of objection, the determination of the fact whether the prerequisites of the data processing are met.

During such restriction, the data processing measures of the indicated personal data may not be carried out, only the storage thereof. In case of the restriction of data processing, the personal data may only be processed in the following cases:

- based on the consent of the data subject
- for the submission, enforcement and protecting of legal claims;
- for the protection of the rights of other natural or legal persons;
- for important reasons of public interest.

We shall inform the Data Subjects of the lifting of the restrictions in advance.

Data portability

Based on a request submitted to any address as indicated in our contact details, the Data Subject is entitled to request the provision of personal data concerning him/her, and processed by us to further use

determined by the Data Subject. Besides that, the Data Subject may also request that we transfer the personal data to another controller indicated by the Data Subject.

This right only covers the personal data provided by the Data Subject and processed for the performance of the contract. There is no possibility for the portability of other data. We shall provide the personal data to the Data Subject in a structured, commonly used and machine-readable format (PDF/XML) and on paper, in a printed format.

We inform the Data Subject that the exercising of this right does not automatically involve the erasure of such personal data from our systems. Besides that, the Data Subject is entitled to contact us and keeping in contact with us again, even following such data portability.

Objection

Based on a request submitted to any address as indicated in our contact details, the Data Subject is entitled to object to the processing of his/her/its personal data for the purposes indicated in Sections 3.1 of this Privacy Policy. In this case, we shall examine whether the data processing is justified by such mandatory legal reasons which take precedence over the interests, rights and freedoms of the Data Subject or which are pertaining to the submission, enforcement or protection of legal claims. Should we determine that such reasons exist, we shall continue processing the personal data. In failure thereof, we shall not process the personal data in the future.