

Privacy notice

(Appendix 1 of Privacy policy)

v1.0	Privacy notice for partners	2/24/2021	
Created by	dr. Barbara Kőrösi (Consact Kft.), István Stikrád		
Status	Final version		
Version control	Original version	v1.0	2/24/2021
	Headquarter address and tax number update	v1.1	1/11/2022

Table of Contents

1. Data controller.....	3
2. Purpose of this notice	3
3. General purpose of data handling.....	3
4. Data handled	3
4.1. Contracting	3
4.2. Invoicing	4
4.3. Contractual relations.....	5
4.4. Contact form on website.....	5
4.5. LinkedIn profile	5
4.6. Forwarding data in order to access procurer’s IT systems	6
4.7. CV for tenders	6
5. Data security.....	7
6. Forwarding data	7
7. Data processors	7
8. Rights of the data subject.....	8
8.1. Right for preliminary information	8
8.2. Right of access	8
8.3. Right to rectification	8
8.4. Right to erasure (“right to be forgotten”).....	8
8.5. Right to restriction of processing.....	9
8.6. Notification obligation regarding rectification or erasure of personal data or restriction of processing	10
8.7. Right to data portability.....	10
8.8. Right to object.....	10
8.9. Automated individual decision-making, including profiling.....	10
8.10. Communication of a personal data breach to the data subject	11
8.11. Right to lodge a complaint with a supervisory authority	11
8.12. Right to an effective judicial remedy against a supervisory authority	11

8.13. Right to an effective judicial remedy against a data controller or data processor11

1. Data controller

Name of the data controller:	endo IT Informatikai Tanácsadó Kft.
Headquarters:	1116 Budapest, Sopron út 64.
Representative:	István Stikrád
Tax number:	13609939-2-43
Company registration number:	01 09 873520
Person responsible for data handling:	István Stikrád
E-mail:	info@endoit.hu
Phone:	+36 1 209 4100
Website:	https://endoit.hu/

2. Purpose of this notice

The aim of this document is to provide clear and accessible information to data subjects on how their data is handled.

When handling your data, we exercise special care to protect your data from unauthorized access. This is a high priority concern for us.

We handle your data with regard to relevant legislation, especially 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) and Hungarian regulations CXII. of 2011 on self-determination rights of information and freedom of information (Infotv.) and XLVII. of 1997 on protection and handling of health-related personal information (Eüak.).

3. General purpose of data handling

Agreements with our customers, partners, fulfilling contracts and handling accounting documents.

4. Data handled

4.1. Contracting

Subjects: Natural persons, who represent a contracted legal entity as an official representative or contact person.

Purpose of data handling: Contracting and fulfillment.

Type of data	Basis for data handling	Retain period
name	Article 6. (1) f) of GDPR Legitimate interest	5 years after contract validity
e-mail address		
phone number		
assignment		
tax number (self-employed)		
bank account number (self-employed)		
registration number of self-employed		
address (self-employed)		
signature		

Process of data handling:

We use the data above for fulfillment of the contract and to facilitate communication for the purpose of contract fulfillment.

If we receive personal information of an employee of a partner organization – typically as contact information – the data is handled on legitimate interest. Legitimate interest of the contracting parties is prioritized over the employee’s self-determination right of personal data because the restriction is necessary and proportional to fulfill their position (NAIH/2018/2570/2/V). A Legitimate Interests Assessment has been carried out to confirm the rightfulness of data handling.

Such personal data is not required, however having to know the data of a contact person is essential for contracting and signing an agreement.

The data may be forwarded to the tax authority (NAV).

4.2. Invoicing

Subjects: Every employee or self-employed person who signs a contract with us.

Purpose of data handling: Handling of documents according to regulation C. of 2000 (Accounting Act) Article 169. sections (1)-(2).

Type of data	Basis for data handling	Retain period
name	Article 6. (1) c) of GDPR Legal obligation	8 years
bank account number		
registration number of self-employed		
address		
tax number		

Process of data handling:

Invoices and related documents issued by our self-employed contractors may contain personal data. We retain these documents for 8 years in accordance with the Account Act.

This information is a required component of these documents. We cannot accept invoices without data mandated by law.

The data is forwarded to our accounting partner (Czefferné Nádazsdi Eleonóra e.v.), and in case of inspection to the tax authority (NAV).

4.3. Contractual relations

Subjects: contact persons of partners (for example the person authorized to sign certification of delivery)

Purpose of data handling: Contacting partners for the purpose of fulfilling contracts.

Type of data	Basis for data handling	Retain period
e-mail address	Article 6. (1) f) of GDPR Legitimate interest	3 months after contract expiration

Process of data handling:

We use the data provided by the partner during contracting to simplify the process of maintaining relationship. E-mail addresses are collected and stored in a sheet and kept as long as necessary for the contractual relation.

When we receive employee personal data of the partner (typically for contacting reasons), we handle such data based on legitimate interest. Legitimate interest of the contracting parties is prioritized over the employee's self-determination right of personal data because the restriction is necessary and proportional to fulfill their position (NAIH/2018/2570/2/V). A Legitimate Interests Assessment has been carried out to confirm the rightfulness of data handling.

Providing this data is not required. To maintain and fulfill a contractual relation however, knowing some personal data of people designated for contacting is necessary.

The data may be forwarded to the tax authority (NAV).

4.4. Contact form on website

Subjects: Persons visiting our website, providing personal data in our contact request form

Purpose of data handling: Contacting prospect customers

Type of data	Basis for data handling	Retain period
name	Article 6. (1) a) of GDPR	Up to 60 days or until the end of business relation
e-mail address	Consent	

Process of data handling:

Personal data provided on the <https://endoit.hu> website's contact form is handled according to the consent of the subject party, exclusively for the purpose of being able to reply to the request.

The subject may withdraw consent at any time without justification, however this has no implications on earlier consent-based data handling.

Data is stored exclusively in electronic form. The website is hosted on servers provided and maintained by MediaCenter Hungary Kft, with whom we have a data processing contract.

4.5. LinkedIn profile

Subjects: Persons following endo IT's LinkedIn profile

Purpose of data handling: Contacting interested potential and existing customers

Type of data	Basis for data handling	Retain period
Data provided on the profile (name, photo, workplace, job, education, expertise, interests, etc.)	Article 6. (1) f) of GDPR Legitimate interest	Information is not stored by endo IT

Process of data handling:

We may use data of subjects following the LinkedIn profile of endo IT for contacting. Currently we don't do such data handling activity, but we have access to profile data of the subjects.

A Legitimate Interests Assessment will be carried out to confirm the rightfulness of data handling in case we opt to perform such contacting or marketing activities.

The subject has the right to object against this data processing (refer to 8.8 for details).

4.6. Forwarding data in order to access procurer's IT systems

Subjects: endo IT's contractors and employees of contractors

Purpose of data handling: Proof of identity to grant IT access

Type of data	Basis for data handling	Retain period
Data requested by the procurer (typically: name, mother's maiden name, place of birth, birth date, address, e-mail address, phone number, e-mail address)	Article 6. (1) f) of GDPR Legitimate interest	Data is not stored, only forwarded

Process of data handling:

In certain cases, procurer's require personal data in order to present proof of identity to grant access to their IT systems.

A Legitimate Interests Assessment has been carried out to confirm the rightfulness of data handling.

4.7. CV for tenders

Subjects: endo IT's contractors and employees of contractors

Purpose of data handling: To correspond to the tender's conditions

Type of data	Basis for data handling	Retain period
name	Article 6. (1) f) of GDPR Legitimate interest	3 years
birth year		
job		
work expertise		
education		
foreign languages		

Process of data handling:

In case it is required by a tender, CVs of participating employees and contractors are forwarded to the procurer.

A Legitimate Interests Assessment has been carried out to confirm the rightfulness of data handling.

The subject has the right to object against this data processing (refer to 8.8 for details).

5. Data security

We apply organizational and technical measures and processes to ensure the safety of personal data handled by us.

Data is protected with appropriate measures against unauthorized access, alteration, forwarding, publication, removal, eradication or damage (accidental or deliberate) as well as becoming inaccessible due to change in technology.

Personal data is only accessible to employees who need such data to complete their job.

To ensure data safety:

- We assess potential risks during planning and operating our IT systems, with the goal to minimize them.
- We monitor potential threats and vulnerabilities (such as computer viruses, security breaches, denial of service attacks, etc.) to timely react with appropriate preventative and defensive measures.
- IT devices and printed information is protected against unauthorized physical access and environmental impact (such as water damage, fire, overvoltage).
- We monitor our IT systems to discover possible problems and incidents.
- To operate our IT systems, we employ only trustworthy people.

6. Forwarding data

Personal data of our partners – except for the cases outlined above – is not forwarded or handed over to other parties. Forwarding of data may happen primarily due to official requests (such as from the tax authority). In some cases it may also be necessary to fulfill contractual obligations, however if this is beyond the purpose of original data handling, we will request an explicit consent from the affected party before the data is handed over to the third party.

Data is not forwarded to other countries or international organizations.

7. Data processors

- MediaCenter Hungary Kft.

Headquarters: 6000 Kecskemét, Sosztakovics u. 3. II/6

Registration number: 03 09 114492

Tax number: 13922546-2-03

Activity: webhosting provider

8. Rights of the data subject

8.1. Right for preliminary information

The subject has the right of getting a clear, concise, and accessible information in written form about data handling. This information must be disclosed latest by the time of acquiring personal data.

If the data controller wants to use collected data for different purposes than originally communicated, the controller must inform the subject about the purposes and all relevant details before carrying out the data processing.

8.2. Right of access

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:

- a) the purposes of the processing;
- b) the categories of personal data concerned;
- c) 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;
- d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- e) 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;
- f) the right to lodge a complaint with a supervisory authority;
- g) where the personal data are not collected from the data subject, any available information as to their source;
- h) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

8.3. 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.

8.4. Right to erasure (“right to be forgotten”)

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b) the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
- c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- d) the personal data have been unlawfully processed;
- e) 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;
- f) the personal data have been collected in relation to the offer of information society services.

Where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

The above shall not apply to the extent that processing is necessary:

- a) for exercising the right of freedom of expression and information;
- b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- c) for reasons of public interest in the area of public health;
- d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing;
- e) for the establishment, exercise or defence of legal claims.

8.5. 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:

- a) 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;
- b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- c) 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;
- d) the data subject has objected to processing; pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

A data subject who has obtained restriction of processing shall be informed by the controller before the restriction of processing is lifted.

8.6. Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

8.7. 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:

- a) the processing is based on consent or on a contract; and
- b) the processing is carried out by automated means.

In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The right shall not adversely affect the rights and freedoms of others. If the right violates this rule, the data controller fulfills its obligations by withholding affected personal data and notifies the data subject about the reasons.

8.8. 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, 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.

8.9. Automated individual decision-making, including profiling

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. This shall not apply if the decision:

- a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- c) is based on the data subject's explicit consent.

In the cases referred to in points (a) and (c), the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

8.10. Communication of a personal data breach to the data subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

8.11. Right to lodge a complaint with a supervisory authority

Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy.

Hungarian supervisory authority:

Nemzeti Adatvédelmi és Információszabadság Hatóság (postal address: 1363 Budapest, Pf. 9., headquarters: 1055 Budapest, Falk Miksa utca 9-11., website: www.naih.hu, phone: 06-1-391-1400, e-mail address: ugyfelszolgalat@naih.hu).

8.12. Right to an effective judicial remedy against a supervisory authority

Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged.

Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

8.13. Right to an effective judicial remedy against a data controller or data processor

Without prejudice to any other administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, each natural or legal person shall have the right to an effective judicial remedy if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

These rights may be exercised on one of our contact channels below in written form, or in person after prior consulting. We strive to reply in the shortest time, but within 15 days most.

Our contact channels:

- Postal mail address: 1507 Budapest, pf 51

- E-mail: info@endoit.hu
- In person: after prior consulting via phone number +36 1 209 4100 or email address info@endoit.hu.

We are unable to provide information regarding personal data via phone because we cannot identify the calling party.