# Privacy Statement and Data Protection Guide

## EasyCON Tanácsadó Kft

1138 Budapest, Váci út 135-139, C, 1st floor

company registration number: Cg. 01-09-193783

# 1. GENERAL PROVISIONS

## 1.1. Purpose of the Privacy Statement and Data Protection Guide

EasyCON Tanácsadó Korlátolt Felelősségű Társaság (hereinafter referred to as: EasyCON Tanácsadó Kft, or the Controller) shall treat personal data confidentially, and shall implement any and all security, technical and organisational measures to guarantee the security of such personal data. This document includes the relevant statement and information, highlighting the rights of data subjects regarding their personal data, and their right to have such data processed in a lawful and secure manner, the protection of such rights as well as their legal remedy options, thus facilitating data subjects exercise their rights.

### 1.1.1 Statement

EASYCON Tanácsadó Kft as the Controller (hereinafter referred to as: EasyCON Tanácsadó Kft or the Controller) acknowledges the provisions of this legal Statement as binding. EasyCON Tanácsadó Kft commits and undertakes that any and all data processing relating to its activities shall comply with the rules, provisions and requirements of its own prevailing Data Protection and Privacy Policy, and Privacy Statement and Data Protection Guide (this document, hereinafter referred to as: the Guide), and those laid down in the applicable legislation.

### 1.1.2 Availability of the Privacy Statement and Data Protection Guide

The Guide, as amended, is available and accessible at any time at https://www.EasyCON.hu/hu/adatvedelmi_es_adatkezelesi_tajekoztato, and a copy can be obtained from the managing director of EasyCON Tanácsadó Kft at request.

## 1.2 The activities performed by the Controller, and the legal basis thereof

### 1.2.1 Personal data processed by the Controller

EasyCON Tanácsadó Kft processes primarily the following categories of personal data of the persons providing such data (e.g. in CVs, business or other offers) on grounds of its existing relationship with them as clients or suppliers, or for the purpose of establishing a contractual relationship with them (hereinafter referred to as: Business Partners):

- their personal data indicated in agreements concluded with Business Partners, offers, quotations, CVs or other documents;
- certain personal data of natural persons indicated in agreements, i.e. natural persons acting on behalf of a Business Partner whilst performing, terminating an agreement, settling accounts relating to an agreement and other transactions;

- video recordings, if the representative of a Business Partner visits the Controller's premises in person.

### 1.2.2 Purpose of processing

The most important evidence and also the guarantee of the lawfulness of all the activities performed by the Controller with the personal data of the data subjects is purpose limitation.

In its capacity as controller, EasyCON Tanácsadó Kft processes personal data in compliance with the provisions of the legislation listed in this Guide. The purpose of processing is to make and conclude, perform business agreements (with clients and suppliers), and to enforce claims arising from an agreement.

Processing always takes place in a scope and for a period of time strictly necessary to achieve the above purposes.

Personal data is transferred to partners providing services to the Controller to the extent necessary to conclude and perform agreements, and to third parties indicated in this Guide, using the (own and external) IT systems of the Controller.

### 1.2.3 Legislative environment

The fundamental principles of processing applied by EasyCON Tanácsadó Kft are consistent and comply with effective laws and regulations on data protection, in particular with those listed below:

- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, hereinafter referred to as: Information Act;
- Act I of 2012 on the Labour Code (Labour Code);
- Act CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing (Research and DM Act);
- Act C of 2000 on Accounting (Act on Accounting);
- Act CVIII of 2001 on certain aspects of electronic commerce and information society services (E-Commerce Act);
- Act C of 2003 on Electronic Communications (E-Communications Act);
- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Business Advertising Activity (Business Advertising Act);
- 1169/2011/EU Regulation of the European Parliament and Council (hereinafter referred to as: GDPR).

EasyCON Tanácsadó Kft wishes to fully comply with the legal requirements of processing personal data, the provisions of the GDPR in particular. This Privacy Statement and Data Protection Guide was prepared in accordance with the GDPR, taking also into consideration the provisions of the Information Act on the right of informational self-determination and on the freedom of information.

#### 1.2.3.1 Territorial scope

The territorial scope of this Guide and the additional documents referred to herein covers any and all processing of personal data carried out at EasyCON Tanácsadó Kft's central unit and all other organisational units, affecting any and all Business Partners.

#### 1.2.3.2 Persons covered

The persons covered by this document include any and all Business Partners who have or intend to enter into a contractual relationship with EasyCON Tanácsadó Kft.

#### 1.2.3.3 Duration

This Guide was prepared in accordance with the provisions of the legislation in effect at the time it was prepared. The Guide may be amended to reflect legislative changes, if there are any, and EasyCON Tanácsadó Kft reserves the right to amend the Guide accordingly at any time. If so, the amended version will be made available on the website in Section 1.1.2 on the working day before it enters into force.

## 1.3 Definitions, basic principles, technical and organisational measures

### 1.3.1 Definitions

- GDPR (General Data Protection Regulation): the General Data Protection Regulation of the European Union;
- 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 transfer, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- 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 Union or Member State law;
- Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- 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;

- Consent of the data subject: 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 breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transferred, stored or otherwise processed;

- Recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
  Third party: 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 authorised to process personal data.
  - Business Partner: A person who has a client or supplier relationship with EasyCON Tanácsadó Kft (even in the absence of a written agreement), or a person who contacts EasyCON Tanácsadó Kft for the purpose of establishing such a relationship with EasyCON Tanácsadó Kft in the future.

### 1.3.2 Basic principles

The Controller states that it processes personal data in accordance with the requirements in this Guide, and complies with the provisions of applicable legislation, considering the following in particular:

- It processes personal data lawfully, fairly and in a transparent manner in relation to the data subject.
- Personal data may only be collected for specified, explicit and legitimate purposes.
- Processing of personal data is lawful and relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Processed personal data are accurate and kept up to date. Personal data that are inaccurate are erased or rectified by the Controller without delay.
- Personal data are kept in a form which permits identification of the data subjects for no longer than is necessary.
- Personal data shall be processed by the Controller in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- The Controller shall apply the principles of data protection to any information relating to an identified or identifiable natural person.

- The Controller shall extend the obligations undertaken through its statement in this Guide to the data processors whose services it uses.

## 1.4 Data security measures

### 1.4.1 Data security

- In its capacity as the controller, EasyCON Tanácsadó Kft shall ensure the security of the personal data it processes. To this end, it shall implement the necessary technical and organisational measures regarding data stored both by means of IT devices and in traditional, paper-based data storage.
- In its capacity as the controller, EasyCON Tanácsadó Kft shall ensure the data protection requirements foreseen in the applicable legislation are duly met.
- In its capacity as the controller, EasyCON Tanácsadó Kft shall take appropriate measures to protect data in particular against unlawful access, change, transfer, publication, erasure or destruction, and against accidental destruction and damage, furthermore against becoming inaccessible due to a change in the technology used.
  In its capacity as the controller, EasyCON Tanácsadó Kft takes into consideration technical progress and the then current state of technology when determining and taking measures to protect data. If there are alternative options to process data, the Controller shall opt for the one that provides higher levels of security for personal data, unless this would represent a disproportionate burden.

### 1.4.2 Protection of IT records

As part of its responsibilities relating to IT security, the Controller shall ensure, in particular:

- protection against unauthorised access, including the protection of software and hardware, and physical protection (access and network protection);
- measures enabling the restoration of data, including regular security back-ups and keeping copies in a secure and separated manner (mirroring, security back-ups);
- protection of data against viruses (anti-virus protection); and
- physical protection of data and data storage devices, including protection against fire, water, lightning and other extreme weather damage, and the possibility of restoration of damage caused by such events (archiving, fire protection).

### 1.4.3 Protection of paper-based records

- In order to protect its paper-based records, the Controller shall take the necessary measures, with regard to physical security and fire protection, in particular.
- Employees and other individuals acting on behalf of the Controller must keep safe and protect the data carriers they use or own, which store also personal data, regardless of the

method of recording such data, protect them from unlawful access, change, transfer, publishing, deletion or destruction, and from accidental destruction or corruption.

## 1.5 General rules of data transfer

- Personal data may only be transferred on the basis of the consent of the data subject, or if authorised by applicable legislation.
- The Controller shall provide data to the authorities on a regular basis with the content, and at the intervals specified in the applicable legislation. In the event of ad hoc data provisions required by law, the Controller must ascertain the legal basis of processing, and, if in doubt, must consult a legal expert.
- Personal data may be transferred only if it has a clear legal basis, its purpose and the recipient of the transfer of data is clearly defined. The transfer of data must always be documented in a manner that the process and the lawfulness of the transfer can be demonstrated. Primarily, the documents requesting or ordering data provision, properly countersigned, and the log entries in the IT systems are used to record and document such transfers.

  The Controller must comply with data transfers prescribed by the applicable legislation. Aside from the above, personal data may be transferred only if the data subject explicitly consented to this. To make sure that such consent is demonstrable, it must be made in writing, if possible. Making such statements in writing may be dispensed with, if the data transfer is of marginal importance in relation to the recipient, the purpose or the scope of the data to be transferred.
- In the event of data transfers requiring the consent of the data subjects, the Controller shall log such transfers so that it can be demonstrated to whom, on what legal basis and for what purpose the data were transferred. Data subjects may consult such data transfer logs, unless the law prohibits such information on the data transfer to be disclosed.

## 1.6 Rights in relation to processing, legal remedy

### 1.6.1 Rights in relation to processing

#### 1.6.1.1Right of information

At the request of the data subject the Controller shall provide information on the data subject's data it manages and the source of such data, the purpose, legal basis and duration of the data management, the name and address of the data processer, the data management activity, and – if the data subject's personal data is forwarded – the legal grounds of the transfer and the recipient of the data. The Controller shall respond to the data subject’s application, and provide this information in writing within the shortest period possible from submission of the application, but within no more than 25 days, using understandable language.

#### 1.6.1.2 Rights to rectification

Data subjects shall have the right to obtain from the Controller the rectification of inaccurate personal data concerning him or her.

#### 1.6.1.3 Right to erasure and the right to object

Data subjects shall have the right to obtain from the Controller the erasure of personal data concerning him or her, unless the Controller is obliged comply with a legal obligation. Data subjects shall be informed about the erasure by the Controller. If processing based on consent is a prerequisite to entering into or maintaining an employment relationship, the Controller shall inform the data subject about this as well as about the envisaged consequences of the processing for the data subject. The Controller may refuse to erase personal data if the processing takes place on the basis of a statutory obligation, or if the processing is necessary to pursue its own legitimate interests. If the Controller refuses to erase personal data, the Controller shall inform the data subject about the reason for doing so.

Data subjects may object to the processing of his or her personal data in accordance with the provisions of the Information Act. Data subjects may also object to automated decision-making.

### 1.6.2 Enforcing rights related to personal data, legal remedy

Data subjects may lodge a request for information about, rectification, erasure or blocking of their personal data primarily with the Controller. If the Controller does not correct, restrict or erase such data at the request of the data subject, it shall state the factual and legal reasons for rejecting the request in writing within no more than 25 days of receipt of the request.

If the request for rectification, blocking or deletion is rejected, the Controller shall inform the data subject about how to seek judicial remedy, and to, alternatively, apply to the Supervisory Authority. In the event of providing information, rectifying, erasure, objection, the Controller shall act in accordance with the provisions of the applicable legislation.

If the rights of the data subject are violated, the competent court for the data subject's place of residence or place of abode shall have jurisdiction. The data subject may enforce their rights pursuant to the provisions of the Information Act or the Hungarian Civil Code.

If the data subject's right to the protection of their personal data are violated, they may take the matter to the Hungarian National Authority for Data Protection and Freedom of Information, and may request the Authority to investigate the matter.

The Controller shall be held liable for the damage caused by unlawful processing as per the applicable laws. The Controller shall be exempt from that liability, if it proves that it is not responsible for the insurmountable causes beyond its control giving rise to the damage. No damages shall be paid, if the damage was caused by the data subject's intentional or grossly negligent conduct. The Controller's general, civil law responsibility is governed by the provisions of the Hungarian Civil Code.

#### 1.6.2.1 The Controller

EASYCON Tanácsadó Kft

1138 Budapest, Váci út 135-139 Building C,

floor 1, www.EasyCON.hu e-mail:

office@EasyCON.hu

Telephone: +36 (1) 781-5818

#### 1.6.2.2 Contact details for the Supervisory Authority:

Hungarian National Authority for Data Protection and Freedom

of Information, postal address: 1530 Budapest, Pf.: 5

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

Telephone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

E-mail: ugyfelszolgalat@naih.hu URL

https://naih.hu

Coordinates: Latitude 47°30'56'' north; Longitude 18°59'57'' east

# 2. SPECIAL PROVISIONS

## 2.1 PROCESSING THE DATA OF BUSINESS PARTNERS

### 2.1.1 Legal basis of processing

Processing is necessary to perform activities with regard to concluding, performing agreements, or activities in relation to concluding agreements, where a Business Partner is one of the Parties, including situations when the data subject acts on behalf of such Business Partner arising from his or her obligations as an employee, obligations arising from any other legal relationship (hereinafter referred to as: performing an agreement).

In its capacity as the Controller, EasyCON Tanácsadó Kft processes personal data on the following legal basis:

#### 2.1.1.1 Concluding, performing or terminating an agreement (legitimate interest)

The personal data of a Business Partner and/or their representative shall be processed by the Controller if necessary for an agreement concluded with, a legal relationship established or to be established with them, in a manner which is proportionate with achieving this purpose.

#### 2.1.1.2 Legal provisions

The legal basis for the processing can be a legal provision, a legal requirement concerning a particular type of agreement or legal relationship, particularly a legal requirement regarding the concluding, maintaining or termination of the agreement in question, or ones governing taxation, social security or accounting issues. (Article 6 b) GDPR)

#### 2.1.1.3 Legal obligations

The processing may be governed by the necessity for the Controller to meet its legal obligations, or the protection of the legitimate interests of the data subject or another natural person (third party). (Article 6 d) GDPR)

#### 2.1.1.4 Consent

The legal basis for processing may be the consent of the data subject. The executive officer of the Business Partner, or the person authorized by such executive officer to do so, may give their consent to processing, necessary for performing an agreement, the lawfulness of which consent shall be guaranteed towards the data subjects (in this case its employees and other natural persons indicated in the agreement or acting on behalf of the Business Partner whilst performing the agreement) by the Business Partner within its own organisation on the condition that they may transfer the personal data only of natural persons whose personal data are protected and safeguarded within their own organisation. (Article 6 (1) a) GDPR)

### 2.1.2Scope of data processed

#### 2.1.2.1 Natural persons who have a contractual relationship

If the Business Partner who has a contractual relationship with the Controller is a natural person, the scope of the data processed shall include: name; e-mail address; telephone number; number of personal identification document; mother's maiden name; date and place of birth; expertise required to conclude a legal relationship; language skills; certificates, diplomas, degrees and examination certificates required to conclude a legal relationship; copies of certificates attesting to the completion of training courses; marital status; number of children; social security number, other personal data necessary for the payment of contractual fees (payroll purposes).

The purpose of processing can include concluding a legal relationship, performing obligations arising from an agreement, enforcing rights and the protection of legitimate interests.

#### 2.1.2.2 Persons other than natural persons who have a contractual relationship

If the Business Partner who has a contractual relationship with the Controller is not a natural person, the scope of the data processed shall include: legal relationship; name; position, e-mail address; telephone number and other necessary contact details of natural persons involved in performing than agreement, or indicated in the agreement or the documents generated whilst performing the agreement.

The purpose of processing can include performing obligations arising from an agreement or a legal relationship, enforcing rights and the protection of legitimate interests.

#### 2.1.2.3 Persons wishing to conclude a contractual relationship, Business Partner

If the Business Partner is a person wishing to conclude a legal or contractual relationship with the Controller, the scope of the data processed shall include: personal data provided in offers, quotations or CVs.

Purpose of data processing: decision-making with regard to concluding a legal relationship or an agreement, offering the possibility of concluding an agreement at a later date, and, to this end, transferring personal data (CVs and related data provided by the data subject) to Business Partners as potential Clients.

Data transfer for this purpose may take place with prior notice given to the data subject to a country in the European Economic Area (hereinafter referred to as: EEA), or to a third country outside the EEA only if the conditions laid down in the GDPR are complied with, and the country in question ensures an adequate level of protection of personal data during processing.

Data transfers to an EEA country shall be deemed as data transfer within Hungary.

The Controller shall process the personal data provided in a CV until withdrawal by the data subject. Given that a Business Partner who wishes to conclude a contractual relationship with the Controller, as a data subject, provides the Controller with its CV and other related personal data voluntarily, its consent to processing its personal data shall be presumed pursuant to Article 4 (11) of the GDPR, and Section 3 (7) of the Information Act.

### 2.1.3 Duration of processing

The Controller processes the personal data necessary to conclude, maintain and terminate a legal relationship, required by statutory provisions relevant to such legal relationships, and necessary to fulfil taxation, social security and accounting obligations at least for a duration prescribed by such relevant laws.

If there is a legal or contractual relationship between the Controller and the Business Partner, the duration of processing is 5 years following the last claim due to the Business Partner arising from that legal or contractual relationship; whereas, pursuant to Section 169 (1.2) a) and b) of the Act on Accounting, it is 8 years in the case of accounting documents generated during the fulfilment of obligations arising from the agreement or any other legal relationship.

In the case of persons falling within the meaning of Section 2.1.2.3 of the Special Provisions, the period of processing lasts until withdrawal of consent by the data subject, but no longer than 6 months if, upon providing his or her personal data, the data subject lodged a request to erase such data.

The Controller ensures that the data the processing period of which has elapsed as explained above are destructed in a secure manner.

### 2.1.4 Special rules of transfer and disclosure of data

#### 2.1.4.1 Information

For the purpose of verifying the lawfulness of data transfer, the Controller provides the data subject with information regarding the data transferred, if necessary.

#### 2.1.4.2 Transfer to a third party

The Controller discloses the Business Partner's personal data to external, third party service providers that assist the Controller's activities as processors, and it is necessary for their work to process such personal data, or a specific range of such data, and that have an appropriate privacy policy and data protection measures in place. Such purposes can include, among others, the auditing of accounts, enforcing and protecting legitimate interests. Such third parties have a contractual obligation prohibiting them from processing, using such personal data beyond the scope of the services provided by them.

In addition, the Controller may transfer personal data to a third party

- in order to enforce or protect its own legitimate interests or those of a Business Partner;
- when complying with a court order or an official order by an authority;
- if lawfully so requested by other government offices and agencies;
- to the new owner, if the ownership of the Controller as a company changes.

### 2.1.5 Designated person responsible for processing

If a data subject has a question, a request or a complaint regarding issues with regard to data processing and data protection, they are encouraged to contact EasyCON Kft using the contact information below:

Telephone: +36 1 781-5818

E-mail: office@EasyCON.hu

## 2.2 Video surveillance at the Controller's premises

### 2.2.1 Purpose and legal basis of operating a video surveillance system

- In order to protect human life, physical well-being of persons and their personal freedom, to protect properties including goods, equipment and assets of significant value, the Controller may operate an electronic surveillance system (hereinafter referred to as: camera system). Cameras operate only at the following premises: EasyCON Office – 1138 Budapest, Váci út 135-139. C. 1st floor.
- The camera system is operated exclusively by the Controller. The Controller appoints a maintenance company with the necessary qualifications, which company guarantees compliance with the data protection rules, to maintain the camera system.
- The cameras are aimed exclusively at areas owned or used by the Controller, and only for specific, lawful purposes.

- The Controller can demonstrate the compliance of the electronic surveillance system in place with the principle of purpose limitation and the obligation to balancing interests as prescribed by Section 4 (1)-(2) of the Information Act.
- The Controller is obliged to install warning signs in the areas where the cameras are installed.

### 2.2.2 Storing video recordings

As a rule, the Controller stores the recordings for 3 working days, storing them for a longer period is permitted in exceptional cases when it is necessary to keep the recordings for a longer period. The Controller must produce evidence to support the reason for doing so.

### 2.2.3 Using video recordings

Handing the video recordings over to a third party (to the police, occupational safety authority) is only permitted in the cases prescribed by law.

Recorded materials may only be viewed if the suspicion of an offence or a crime arises, or if an occupational accident happens.

Video recordings may be used as evidence in court or before another authority. The digitally recorded materials cannot be accessed from external systems, back-ups or copies may only be made of them only in the cases listed in the relevant laws, e.g. for the purposes of criminal proceedings.

The security cameras operate on a continuous basis. It is prohibited to switch them off, or to hinder recording in any way.

### 2.2.4 Viewing video recordings

The persons authorised to view, make back-ups of, supervising the erasure of recordings made by the cameras and moved to storage include:

- managing director
- system administrator in the presence of the managing director.

The reason and the date of viewing such recordings, and the name of the person authorised to view them must be stated in a report.

When viewing recordings made with regard to a visit by a Business Partner or an Employee, the right to be present at the viewing must be ensured to the representative of the given Business Partner or Employee, respectively, and the statements made by the representative or the Employee, if any, must be included in the report.

Data subjects may request information about the processing of the recordings.

The persons authorised to view the live images broadcast continuously by the cameras include:

- managing director
- system administrator

### 2.2.5 Data security measures

The screen used to view the live images and the recordings is installed in a way to make it impossible for any person other than those authorised to view them whilst the images or recordings are broadcast or shown.

Monitoring live images and the viewing of stored recordings may take place only to identify unlawful acts, and to put in place measures necessary to stop such acts.

The images broadcast by the cameras may not be recorded using a device other than the central recording unit.

Access to the stored recordings may only take place in a secure manner, identifying the person of the Controller. The viewing of stored recordings and making back-ups thereof must be documented. Access to the stored recordings must be terminated immediately if the reason for eligibility discontinues.

Video recordings are stored on a dedicated target hardware. The device is kept is a physically closed space, access to the system requires authentication with a username and password.

If an unlawful act is detected, the necessary measures must be taken to block the recording made of the act, and to start the necessary official procedure without any delay, and the authority in question must be informed that a video recording was made of the act.

Warning information must be given at the entrances and in areas used by employees and other visitors about the fact that a video surveillance system is in place and in operation.

# 3. Duration

This Guide was prepared in accordance with the legislation in effect on 31 January 2019, and this version entered into force on the same day.

Budapest, 30 January 2019

EASYCON Tanácsadó Kft

……

Managing Director Géza Balázs