

iContrAll Intelligent Building Electronics
Limited-liability Compony

DATA MANAGEMENT AND PRIVACY POLICY

Contents

1.) Data controller's information	5
2.) Relevant legislation	5
3.) Definations.....	5
4.) Data management principles.....	6
5.) RECORDING DATA, REGISTRATION, MAILING, COOKIES	7
5.1. Data Controller	7
5.2. Newsletter.....	8
5.3. Logging the server	8
5.4. Cookie management.....	9
5.5. Contact on the site.....	9
5.6. Records.....	11
6.) Data asset map.....	11
6.1. Visitor status.....	11
6.2. Visitor status	11
7) Personal and special data processed by the data controller, their source, purpose, legal basis and duration of the data processing:.....	12
8.) The scope of data to be provided during the performance of the contract, the category of data, the source of the data, as well as the purpose of the data processing and the lawfulness of the data processing (legal basis)	13
9.) Management of personal data concerning children	14
10.) The range of persons entitled to access personal data, data processing.....	14
11.) Rights of the Data Subject	15
11.1. Access to personal and special data.....	15
11.2. Correction of managed data	16
11.3. Delete managed data (right to forget), lock.....	16
11.4 . Restrict managed data	17
11.5. Notification obligation related to the correction or deletion of personal data or restrictions on data processing	17
11.6. Right to protest.....	17
12.) Data security	18
13.) Handling and reporting privacy incidents.....	18
14.) Enforcement options	19

14.1. Icontrall internal enforcement 19

14.2. Enforcement before Naih 19

14.3. Judicial enforcement..... 19

14.4. Compensation and damages 20

15. Document data 20

16. Version tracking..... 20

iContrAll Intelligent Building Electronics Limited Liability Company (registered office: 2120 Dunakeszi, Eszék utca 2., Cgj .: 13-09-134920, hereinafter: **Data Controller**) complies with these Data Management and Data Protection Regulations (hereinafter: **the Regulations**) in order to fully comply with the applicable Hungarian legal provisions.). The Data Controller shall provide the personal and special data and information provided by the person who comes into contact with him / her in any way and who may establish any legal relationship after the contact (hereinafter: **the Data Subject**) in accordance with the applicable Hungarian data protection legislation (especially, but not limited to Act CXII of.,). In drafting the provisions of the Regulation, the Data Controller took into account in particular the European Parliament and Council Regulation 2016/679. (hereinafter: **GDPR**).

Prior to the commencement of data processing, the Data Controller shall provide information on the facts related to the processing of personal and special data provided with the voluntary consent of the Data Subject, the purpose, legal basis, duration of the data processing, the scope of personal data and data processing. These Regulations also cover the data subjects' rights related to data processing and legal remedies.

The Data Controller emphasizes that the processed data is stored securely, records are kept securely, the Data Subject is informed about the stored data upon request and the Data Subject may request the deletion of the data at any time, free of charge and without justification, at info@icontrall.com.

These regulations are available free of charge to anyone at the Data Controller's headquarters (2120 Dunakeszi, Eszék utca 2.) and on their website: www.icontrall.com.

1.) Data Controller's information

The data manager is **iContrAll Intelligent Building Electronics Limited Liability Company**

Headquarters:	2120 Dunakeszi, Eszék utca 2.
Cgj.:	13-09-134920
Tax number:	12412240-2-13
Registry Court:	Budapest Környéki Törvényszék Cégbírósága
Represented by:	Kovács Zoltán és Kurucz Máté Dániel ügyvezetők
Privacy Officer:	Kovács Zoltán
Marketing Officer:	Kurucz Máté Dániel (Google Ads kampány) és Kovács Zoltán
E-mail address:	info@icontrall.com
Phone number:	+36 1 369 3939

2.) Relevant legislation

The data controller undertakes to carry out its activities in accordance with the Hungarian legislation in force at any time. At the time of entry into force of these Regulations, these include, but are not limited to:

- 2008 XLVIII. Act on the Basic Conditions and Certain Restrictions of Commercial Advertising (hereinafter: the Commercial Advertising Act).
- 2005 XC. Electronic Freedom of Information Act
- Act C of 2003 on Electronic Communications (specifically Section 155)
- 16/2011. s. Opinion on the EASA / IAB Recommendation on Best Practices for Behavioral Online Advertising
- Recommendation of the National Authority for Data Protection and Freedom of Information on data protection requirements for prior information
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46 (hereinafter referred to as GDPR)
- 2011 CXII. Act on the Right to Information Self-Determination and Freedom of Information.
- Regulation (EC) No 2016/687
- 1997 XLVII. Act on the Processing and Protection of Health and Related Personal Data

3.) Definitions

2011 CXII. pursuant to Section 3 of the Act

1. *Data subject*: Any natural person identified or identifiable, directly or indirectly, on the basis of personal data;
2. *Personal data*: data which can be contacted with the data subject, in particular the name, identification mark and knowledge of one or more physical, physiological, mental, economic, cultural or social identities of the data subject, and the conclusion which can be drawn from the data concerning the data subject;
3. *Special data*:
 - Personal data concerning racial origin, membership of a national or ethnic minority, political opinion or party affiliation, religious or other beliefs, membership of an advocacy organization, sex life,
 - Personal data on health status, pathological passion and personal data on crime;
4. *Personal data relating to a criminal offense*: personal data obtained during or before criminal proceedings in connection with a criminal offense or criminal proceedings, at bodies authorized to conduct criminal proceedings or to detect criminal offenses, and at the organization responsible for enforcing a criminal offense;
5. *Data of public interest*: information or knowledge recorded in any way or form that is not covered by the concept of personal data, regardless of the concept of personal data, regardless of the concept of personal data, regardless of the concept of personal data. information on the manner in which it is

- handled, whether independent or aggregate, in particular information on competence, competence, organizational structure, professional activity, its effectiveness, the types of data held and the legislation governing its operation, as well as information on management and contracts;
6. *Public data in the public interest*: all data not covered by the concept of data of public interest, the disclosure, disclosure or making available of which is required by law in the public interest;
 7. *Consent*: the voluntary and explicit expression of the will of the data subject, based on adequate information and giving his or her unambiguous consent to the processing of personal data concerning him or her, in full or in part;
 8. *Objection*: a statement by the data subject objecting to the processing of his or her personal data and requesting the termination of the processing or the deletion of the processed data;
 9. *Data controller*: any natural or legal person, or any entity without legal personality, who alone or jointly with others determines the purposes for which the data are processed, makes decisions and implements data processing (including the means used), or with a data controller entrusted by him executes;
 10. *Data management*: any operation or set of operations performed on data, regardless of the procedure used, in particular the collection, recording, recording, systematisation, storage, alteration, use, interrogation, transmission, reconciliation or linking, blocking, erasure and destruction of , and to prevent further use of the data, the taking of photographs, sound or images and the recording of physical characteristics capable of identifying the person (eg fingerprint or palm print, DNA sample, iris image);
 11. *Data transfer*: making the data available to a specific third party;
 12. *Disclosure*: making the data available to anyone;
 13. *Data erasure*: making data unrecognizable in such a way that it is no longer possible to recover it;
 14. *Data marking*: identification of the data in order to distinguish it;
 15. *Data blocking*: the restriction of the further processing of the data to identify them for a definitive or specified period;
 16. *Destruction of data*: the complete physical destruction of the data carrier;
 17. *Data processing*: the performance of technical tasks related to data management operations, regardless of the method and means used to perform the operations and the place of application, provided that the technical task is performed on the data;
 18. *Data processor*: a natural or legal person or an organization without legal personality who, on the basis of a contract concluded with a data controller, including the conclusion of a contract pursuant to a legal provision, processes data;
 19. *Data controller*: the body performing a public task which has produced data of public interest to be published compulsorily by electronic means, or in the course of the operation of which this data has been generated;
 20. *Informant*: the body performing a public task which, if the data controller does not publish the data itself, publishes the data provided to it by the data controller on a website;
 21. *Data set*: the totality of the data managed in one register;
 22. *Third party*: any natural or legal person, or any entity without legal personality, who is not the data subject, controller or processor;
 23. *EEA State*: a Member State of the European Union and another State party to the Agreement on the European Economic Area, as well as a State of which the European Union and its Member States and a State not party to the Agreement on the European Economic Area are nationals, Enjoys the same status as a national of a State party to the Agreement on the European Economic Area;
 24. *Third country*: any non-EEA state.

4.) Data management principles

- a) the voluntary informed consent of the data subject in accordance with **Article 6 (1) (a) of the GDPR**;
- b) in accordance with **Article 6 (1) (b) of the GDPR**, the processing is necessary for the performance of a contract to which one of the parties is a party;
- c) the processing is necessary to fulfill a legal obligation to the controller under **Article 6 (1) (c) GDPR**;
- d) the processing is necessary for the protection of the legitimate interests of the controller or of a third party in accordance with **Article 6 (1) (f) GDPR**;

(e) Act CVIII of 2001 on certain aspects of electronic commerce services and information society services. Act (hereinafter: **Elkertv.**) **13 / A. §** - the data management permit provided by the user, according to which the natural personal identification data of the Users (name, birth name, mother's birth name, place and time of birth) and address can be processed without the consent of the User, the establishment and definition of the contract. The address of the User's natural personal data and the data on the date, duration and location of the use of the service for the provision of the information society-related service may be processed without the consent of the User for the purpose of modifying, monitoring the fulfillment of the for the purpose of invoicing the fees arising from the contract.

The declaration of an incapacitated and incapacitated minor requires the consent of his or her legal representative, except for those parts of the service where the declaration is intended for mass registration in everyday life and does not require special consideration.

Personal and special data may only be processed for a specific purpose, in order to exercise a right and fulfill an obligation. This purpose must be met at all stages of data management.

Only personal and special data that are necessary for the realization of the purpose of data processing, suitable for the achievement of the purpose, may be processed only to the extent and for the time necessary for the realization of the purpose.

Personal and special data may only be processed with informed consent.

In these Regulations, the Data Controller shall inform the data subject in a clear, comprehensible and detailed manner of all facts related to the processing of his / her data, in particular the purpose and legal basis of the data processing, the person authorized to process the data and the data processing. The information shall also cover the data subject's rights and remedies in relation to data processing.

In this regard, the Data Controller provides more information at <http://www.icontrall.com/adatvedelem.html>.

Personal and special data processed by the data controller shall meet the following requirements:

- Their admission and treatment is fair and lawful;
- Accurate, complete and timely;
- The manner in which they are stored is such that the data subject can be identified only for the time necessary for the purpose of storage.

In this context, the data controller shall state that it shall not use a general and uniform personal identification mark in respect of the recorded data without any restrictions.

The data controller declares that personal and special data will only be transferred and the various data processing will be combined only if the Data Subject has consented to it or is permitted by law, and if the conditions for data processing are met for each personal data.

5.) RECORDING DATA, REGISTRATION, MAILING, COOKIES

5.1. Data Controller

5.1.1. **By registering** at <http://www.icontrall.com/>, the Data Controller requests the following information:

- e-mail address
- first and last name
- phone number

5.1.2. The Data Controller **requests the following data for concluding contracts and bidding:**

- e-mail address
- first and last name

iContrAll Ltd. Privacy and privacy policy

- phone number
- billing name,
- billing address
- the name of the operational contact person (who is entitled to make an administrator and a legal declaration during the period of work),,
- e-mail address of operational contact,
- phone number of operational contact,
- place of performance (exact address of the property),
- floor area of the property
- expected date of handover of the work area (end of electrical installation)

5.2. Newsletter

The data controller keeps the listed data in its records and uses them for communication and promotional mail. The data subject may request the termination of the sending of these letters to the Data Controller at any time, free of charge and without justification, by sending an e-mail to info@icontrall.com.

The data controller does not send an electronic direct marketing message directly to the Data Subject by e-mail. The legal basis for sending a data controller letter is a legitimate business interest under Article 6 (1) (f) GDPR. The data subject shall send the e-mail to the Data Subject with the consent of the Data Controller during the registration pursuant to Article 6 (1) (a) of the GDPR.

5.3. Logging of server

When you visit www.icontrall.com, the web server does not record user data.

Logging data management for external data handlers:

The HTML code of the portal contains links to and from an external server independent of iContrall Kft. The external data server is directly connected to the user's computer. The data controllers of these links collect user data (eg IP address, browser, operating system data, mouse pointer movement, address of the page visited and the time of the visit) due to the direct connection to their server and the direct communication with the data subject's browser. according to.

The purpose of data management: to ensure the normal operation of the server server, to verify the system activities

Legal basis for data processing: the Data Controller has a legitimate interest in the personalized service of users (Article 6 (1) (f) GDPR).

Type of personal data processed: identification number (stored on the user's computer by means of cookies), the address of the page visited, the date and time of the visit, the details of the user's computer and browser, the screen resolution, the language settings, the identification number formed from the IP address of the user's computer.

Duration of data processing: 30 days.

Common data controller (s): None.

Data processor (s):

Name	headquarters	Data processing task
iContrAll Ltd.	2120 Dunakeszi, Eszék utca 2.	Technical execution of log analyzes
Magyar Hosting Ltd.	1132 Budapest Victor Hugo u. 18-22.	Providing online hosting
DigitalOcean LLC.	101 Avenue of the Americas, 10th Floor New York, NY 10013	Server provider*

* In connection with the management of iContrAll data, the data stored by the designated server provider is located on a server located in the European Union (Frankfurt am Main, Germany).

5.4. Cookie management

When using its service, the data controller uses small programs called **cookies** and similar technologies on the devices to help with identification, to help identify the data so that you do not have to re-enter it all the time to improve the user experience, increase the security of your service, efficiency. If the browser returns a previously saved cookie, the data controller handling the cookie has the option to link the user's current visit to the previous ones, but only for their own content.

This data is not provided by the Data Subject, but is collected from the Data Subject by the Data Controller and / or its subcontractor or employee during the use of the website, social media pages (Facebook, Instagram, LinkedIn).

This includes the IP address of the Data Subject, the type of devices used by the Data Subject to browse the online interfaces of the Data Controller, the operating system, the type of browser used and other technical characteristics, the amount of time spent on each of our websites, the number and location of clicks.

The data controller also employs small programs that remember when the data subject last logged in to the online interfaces, which store their login information so that they can recognize it the next time they return and make it faster to log in.

The purpose of data management is to identify the affected users, to differentiate them, to identify the current session of the users, to store the data provided during it, to prevent data loss, and to use web analytics.

Legal basis for data processing: the Data Controller has a legitimate interest in the personalized service of data subjects (Article 6 (1) (f) GDPR).

The scope of the data processed: identification number, date, time and activities performed at www.icontrall.com.

Duration of data processing: 16 months.

Data processor (s):

Name	headquarters	Data processing task
iContrAll Kft. (Kovács Zoltán)	2120 Dunakeszi, Eszék utca 2.	Website developer Perform backups on the website, perform development and database related tasks
Magyar Hosting Kft.	1132 Budapest Victor Hugo u. 18-22.	Providing online hosting

Cookies with an exact validity period (permanent) until they are deleted, but no later than the expiry date stored on your computer.

The data subject can delete the cookie from his or her own computer or disable the use of cookies in his or her browser.

A cookie is a packet of alphanumeric information sent by a web server that is stored on a user's computer and stored for a predetermined period of time. The use of cookies makes it possible to query certain data of the visitor and to monitor the use of the Internet. With the help of cookies, the interests of the Affected User, the usage habits of the Internet and the history of website visits can be precisely determined. Because cookies act as a kind of tag with which the website can recognize the visitor returning to the page, their application can also store a valid username and password on the given page. If the user's browser returns a previously saved cookie to the hard drive during the visit to the website, the data controller who sent it may link the current visit to the previous one, but since the cookies are linked to the domain, it is only able to do so for its own content. Cookies are not in themselves capable of identifying the Affected User, they are only used to identify the visitor's computer.

5.5. Contact on the site

The Data Controller is in order to facilitate communication from the user in order to provide customized service Provides an easy-to-use and secure interface for contact and more to provide information and answer any questions you may have.

iContrAll Ltd. Privacy and privacy policy

The Data Controller requests the data only for the purpose of contact, it does not transfer them to third parties, no further not used for marketing purposes.

The purpose of data management is to contact the data subject by telephone and e-mail.

Legal basis for data processing: consent-based data processing under (Article 6 (1) (a) GDPR).

The scope of the managed data: name, telephone number, e-mail address, company name.

Duration of data processing: data provided by the data subject until revoked, but not later than one year

Data processor (s):

Name	headquarters	Data processing task
iContrAll Kft.	2120 Dunakeszi, Eszék utca 2.	Website developer
Magyar Hosting Kft.	1132 Budapest Victor Hugo u. 18-22.	Providing online hosting, provision of mail services, storage of electronic mail and documents

The length of the retention period was defined by the legitimate interest of the Data Controller and the Data Subject to be able to verify the communication and the related costs in the event of an official investigation.

If the Data Subject enters into a contract with the Data Processor, the data management shall be modified as follows:

Purpose of data management: To operate the business based on the written agreement of the contracted partners.

Legal basis for data processing: data processing based on the performance of a contract and a legal obligation (Article 6 (1) (b) and (c) GDPR).

Scope of data processed: surname and first name, telephone number, e-mail address, company name; tax number, company registration number, billing address, delivery address, contact, identification of the person transferring and receiving, other technical data necessary for the performance of the task (eg doorbell number).

Duration of data processing: the data provided by the data subject is stored for eight years in accordance with the Accounting Act appropriately.

5.6. Customer correspondence

The Data Controller will delete all e-mails received by him / her, together with the sender's name, e-mail address, date and time data and other personal data provided in the message, **up to 10 years after the communication**.

In addition, all of the emails we send out contain the following information:

„iContrAll Kft. is the 2016/679 EU-GDPR, and the amended 2011 CXII. of the data management information prepared on the basis of the relevant provisions (www.icontrall.com under "Privacy") 5.6. process the personal data concerned in its electronic mail as defined in.”

The purpose of data management is to provide contact and communication related to the business process through electronic mail.

Legal basis for data processing: data processing based on consent for the use of the service and in order to ensure the legitimate interest of the data controller in order to be verifiable.

The type of personal information processed: the sender's name, telephone number, e-mail address, date values and other time information, and other personal information and information provided in the message.

Duration of data management: 10 years.

Data processor (s):

Név	headquarters	Data processing task
iContrAll Kft.	2120 Dunakeszi, Eszék utca 2.	A data controller using an electronic mail system
Magyar Hosting Kft.	1132 Budapest Victor Hugo u. 18-22.	provision of correspondence services and storage of electronic mail and documents

iContrAll Ltd. Privacy and privacy policy

The length of the retention period was defined by the legitimate interest of the controller and the processor in verifying the communication and the related costs in the event of an official investigation.

5.7. Records

The Data Controller **requests contact information** from the user for one-time electronic information and to provide a customized service. The data is recorded in an easy-to-use and secure interface / registry provided by Microsoft in the Office365 (EXCEL) environment. The primary purpose of the contact is to provide additional information and answer any questions you may have.

The data controller requests the data only for the purpose of contact, does not pass them on to third parties, and does not use them for further marketing purposes. The controller shall make a specific request to the data subject in order to use his or her data for other purposes. The data subject may request the Data Controller at any time, free of charge and without justification, by sending an e-mail to info@icontrall.com.

The purpose of data management is to contact the data subject by telephone and e-mail

Legal basis for data processing: consent-based data processing under (Article 6 (1) (a) GDPR).

The scope of the managed data: name, telephone number, e-mail address, company name

Duration of data processing: data provided by the data subject until revoked, but not later than one year

Data processors:

Név	headquarters	Data processing task
iContrAll Kft.	2120 Dunakeszi, Eszék utca 2.	Creator of the data entry interface (FORM)
Magyar Hosting Kft.	1132 Budapest Victor Hugo u. 18-22.	provision of correspondence services and storage of electronic mail and documents

The length of the retention period was defined by the legitimate interest of the controller and the processor in verifying the communication and the related costs in the event of an official investigation.

6.) Data asset map

The Services and the supply of products may be used by the Data Subject according to the following grouping, during which the Data Controller handles personal data.

The scope of this data managed and recorded and further information on its handling is provided in sections 7 and 8.

6.1.Visitor status

If the Data Subject merely finds information and collects information on the website, he / she will use the website service as a visitor (hereinafter: "Visitor"). As a Visitor, any personal data on the basis of which the Visitor could be identified will not be in the possession of the Data Controller, in which case it will not store data about the Visitor. However, when you visit (also) we create a technical ID, as described in 5.4. the so-called cookie / cookie detailed under.

6.2. Customers status

If you order the design, construction or programming of the Affected System, as well as the possible extension of this system in the future, it is necessary to provide the Data Controller with the personal data explained below.

7) Personal and special data processed by the data controller, their source, purpose, legal basis and duration of the data processing:

Data	data source	Purpose of data management	Legal basis for data management	Duration of data management
name	Affected	(a) registration (b) identification c) contact b) sending mail and system messages	-the consent of the person concerned GDPR Article 6 (1) a) and f) - Elkertv. 13 / A. §	Until withdrawal of consent
e-mail address	Affected	(a) registration (b) identification c) contact b) sending mail and system messages	-the consent of the person concerned GDPR Article 6 (1) a) and f) - Elkertv. 13 / A. §	Until withdrawal of consent
password	Affected	(a) registration (b) identification c) contact b) sending mail and system messages	-the consent of the person concerned GDPR Article 6 (1) a) - Elkertv. 13 / A. §	Until withdrawal of consent
address	Affected	(a) registration (b) identification c) contact b) sending mail and system messages	the consent of the person concerned GDPR Article 6 (1) a)	Until withdrawal of consent
phone number	Affected	(a) registration (b) identification c) contact b) sending mail and system messages	the consent of the person concerned GDPR Article 6 (1) a)	Until withdrawal of consent
photo and videorecords	Affected	a) promotion	- the consent of the person concerned GDPR Article 6 (1) a)	Until withdrawal of consent

8.) The scope of data to be provided or managed during the performance of the contract, the data category, the source of the data, as well as the purpose of the data processing and the legality of the data processing (legal basis)

Data	data source	Purpose of data management	Legal basis for data management	Duration of data management
1. billing first name and last name*	specified by affected	(a) customer identification b) providing communication (c) establishing, defining, amending and monitoring the performance of the contract d) in case of establishment of a contractual relationship, invoicing of the resulting fees (eg purchase price, contractor fee) (e) the prevention of possible claims and fraud	-performance of the contract Article 6 GDPR -legitimate interest Article 6 GDPR - fulfillment of a legal obligation Article 6 of the GDPR	Until withdrawal of consent Until the termination of the contract 2000. tv tv. § 169 for 8 years
2. billing address	specified by affected	(a) customer identification b) providing communication (c) establishing, defining, amending and monitoring the performance of the contract d) in case of establishment of a contractual relationship, invoicing of the resulting fees (eg purchase price, contractor fee) (e) the prevention of possible claims and fraud	-performance of the contract Article 6 GDPR -legitimate interest Article 6 GDPR - - fulfillment of a legal obligation Article 6 of the GDPR	Until withdrawal of consent Until the termination of the contract 2000. tv tv. § 169 for 8 years
3. surname and first name of the operational contact *	specified by affected	(a) customer identification b) providing communication (c) establishing, defining, amending and monitoring the performance of the contract d) in case of establishment of a contractual relationship, invoicing of the resulting fees (eg purchase price, contractor fee) (e) the prevention of possible claims and fraud	-performance of the contract Article 6 GDPR -legitimate interest Article 6 GDPR - - fulfillment of a legal obligation Article 6 of the GDPR	Until withdrawal of consent Until the termination of the contract 2000. tv tv. § 169 for 8 years
4. e-mail address of operational contact*	specified by affected	(a) customer identification b) providing communication	-performance of the contract Article 6 GDPR	Until withdrawal of consent

iContrAll Ltd. Privacy and privacy policy

		(c) establishing, defining, amending and monitoring the performance of the contract	-legitimate interest Article 6 GDPR	Until the termination of the contract
5. The address of the property to which the system requests installation / installation *	specified by customer	(a) customer identification b) providing communication	performance of the contract Article 6 GDPR -legitimate interest Article 6 GDPR	Until withdrawal of consent Until the termination of the contract
6. A list of assets connected to the system in the property	Specified by end user	(a) system operation, troubleshooting, recovery after possible damage (b) to ensure continuous, safe use	performance of the contract Article 6 GDPR -legitimate interest Article 6 GDPR	Until the termination of the contract
7. User settings for the system in the property	Specified by end user	(a) system operation, troubleshooting, recovery after possible damage (b) to ensure continuous, safe use	performance of the contract Article 6 GDPR -legitimate interest Article 6 GDPR	Until the termination of the contract
8. Log files for using the system built in the property	Data generated during use, based on data provided by the End User	(a) system operation, troubleshooting, recovery after possible damage (b) to ensure continuous, safe use	performance of the contract Article 6 GDPR -legitimate interest Article 6 GDPR	Until the termination of the contract

In order to use the contracted services and purchase the iContrAll products, the information marked with * in the table above is essential for the conclusion of the contract, and this information is a prerequisite for concluding the contract and is therefore mandatory.

9.) Management of personal data concerning children

The processing of data relating to children is lawful under the GDPR if the child has reached the age of 16, in the case of a child under the age of 16, the processing of his or her personal data is lawful only if and to the extent that the child has parental custody of the child (eg parent, guardian, other legal representative).

10.) The range of persons entitled to access personal data, data processing

10.1. Personal data may be accessed by the Data Controller or its subcontractors or persons with an employment relationship with the Data Controller in accordance with the applicable legislation.

10.2. Data management subcontractors, data processors:

In addition to the data processors highlighted above, the Data Controller shall transmit the personal data specified in clauses 7 and 8 to the following companies, and these companies shall have access to the data registered by the Data Controller for the following purposes, which are absolutely necessary to achieve this purpose:

iContrAll Ltd. Privacy and privacy policy

1. **Billing program:** **Budapest Asset Financing Ltd.** (1138 Budapest, Váci út 193., phone number: +36 20 444-4202, e-mail address: info@bupa.hu, website: bupa.hu, tax number: 10446173 -4-41, comp. num.: 01-10-041505, represented by Dr. József Kornél Barna, Chief Executive Officer), who invoices the Data Controller.

2. **Accounting office:** **GP-Conto Ltd.** (2163 Vácrátót, Petőfi tér 10., branch office: 1132 Budapest Victor Hugo u. 11-15. 115511, telephone number: +36 20 329 2389, accountant: Kornélia Gulyás, contact e-mail address: e-mail address: gulyas.kornelia@gpconto.hu), which performs the accounting of the Data Management Company.

3. **Lawyer:** **dr. Péter Soós individual lawyer** (szh.:1055 Budapest Szent István krt. 13. III. Em. 2 / b., Telephone number: +36 1 788 0187, e-mail address: peter.soos@avocat.hu, Chamber of Registry: Budapest Bar Association), who e.g. performs receivables management.

The Data Controller / Data Processor enters into a data controller / data processor contract with the service provider indicated above / the companies' own terms and conditions stipulate that the Data Controller / Data Processors undertake and provide a guarantee for the protection of personal data. In the latter case, the Data Controller does not guarantee and expressly excludes its liability for the existence, compliance with and enforcement of data protection rules in accordance with the legislation in force at the data processors.

Microsoft Inc. and its affiliates are listed in the European Commission's **GDPR Article 45** Compliance Decision and Commission Implementing Decision 2016/1260, as well as the US-EU Privacy Shield List (<https://www.privacyshield.gov/>) list), ie the transfer to this country does not constitute a transfer to a third country outside the European Union and does not require the specific consent of the data subjects, and the transfer to that country is permitted under Article 45 of the GDPR. This company undertook to comply with the GDPR.

Based on the authorization of the court, the prosecutor, the investigating authority, the infringement authority, the administrative authority, the National Data Protection and Freedom of Information Authority or other bodies, they may contact the Data Controller to provide information, disclose data or make documents available.

The Data Controller shall disclose personal data to the authorities only if and to the extent strictly necessary to achieve the purpose of the request, provided that the authority has indicated the exact purpose and scope of the data.

The data controller does not transfer personal data to a third country that is not a party to the GDPR, within the meaning of the GDPR, only to the data controllers / processors specified in these data processing regulations, as detailed therein.

No Data Protection Officer has been appointed by the Data Controller in accordance with the provisions of the GDPR Regulation.

No profiling or automatic decision-making is performed based on the data managed by the data controller.

11.) Rights of the Data Subject

The Data Subject may request the Data Controller to provide information on the processing of the Data Subject's personal data, the Data Subject may request the correction of his or her personal data and may request the deletion or blocking of his or her personal and special data, except for mandatory data processing.

The Data Subject may request the Data Controller to access, correct, delete or restrict the processing of personal and special data concerning him or her. In addition, you have the right to receive personal and special data concerning you provided to the Data Controller in a structured, widely used, machine-readable format and to transfer this data to another data controller (right to data portability). The data subject shall also have the right to withdraw his or her consent to the processing at any time, without prejudice to the lawfulness of the data processing prior to the withdrawal.

Below is a brief description of each of the data subject's rights:

11.1. Access to personal and special data

At the request of the Data Subject, the Data Controller shall provide information on whether the Data Controller continues to process data concerning his / her personal and special data and, if so, shall grant him / her access to the personal and special data and inform him / her of the following information:

- the purpose (s) of the data processing;
- the types of personal and / or special data involved in the processing;
- in the case of transfers of personal and / or special data of the Data Subject, the legal basis and recipient (s) of the transfer;
- the planned duration of the data processing;
- the rights of the Data Subject in relation to the rectification, erasure and restriction of the processing of personal data and the protest against the processing of personal data;
- the possibility to apply to the Authority;
- the source of the data;
- the names and addresses of the data processors and their activities related to data management.

The Data Controller shall make a copy of the personal and special data subject to data processing available to the Data Subject free of charge. The Data Controller may charge a reasonable fee based on administrative costs for additional copies requested by the Data Subject. If the data subject has submitted the request by electronic means, the information shall be provided in a widely used electronic format, unless otherwise requested by the data subject.

The data controller is obliged to provide the information at the request of the Data Subject without undue delay, but no later than within 30 days from the submission of the request. The Data Subject may submit a request for access at the contact details set out in point 1.

11.2. Correction of managed data

The Data Subject may request from the Data Controller (at the contact details specified in point 1) the correction of inaccurate personal data or the supplementation of incomplete data, taking into account the purpose of the data processing. The data controller shall carry out the correction without undue delay.

11.3. Delete managed data (right to forget), lock

The Data Subject may request that the Data Controller delete personal or special data concerning him or her without undue delay, and the Data Controller shall delete the personal or special data relating to the Data Subject without undue delay if any of the following reasons exists:

- (a) personal data are no longer required for the purpose for which they were collected or otherwise processed;
- (b) the data subject withdraws his or her consent and there is no other legal basis for the processing;
- (c) the Data Subject objects to the processing of his / her personal data;
- (d) personal data have been processed unlawfully;
- (e) personal data must be deleted in order to fulfill a legal obligation to which the controller is subject under applicable Union or Member State law;
- (f) personal data have been collected in connection with the provision of information society services to children.

If the Data Controller has disclosed (made available to a third party) personal data and is obliged to delete it in accordance with the above, taking into account the available technology and the costs of implementation, it must take reasonable steps and measures to inform the personal data concerned. data controllers that the Data Subject has requested the deletion of links to the personal data in question or of a copy or duplicate of such personal data.

Personal or special data need not be deleted if data processing is required:

- to exercise the right to freedom of expression and information;

- in order to fulfill an obligation under EU or Member State law governing the processing of personal data or to perform a task carried out in the public interest or in the exercise of a public authority conferred on the Data Controller;
- in the public interest in the field of public health;
- for the purpose of archiving in the public interest, for scientific and historical research purposes or for statistical purposes, where the right of erasure would make this processing unlikely to be impossible or seriously jeopardized; obsession
- to file, enforce or defend legal claims.

11.4. Restrict managed data

The Data Subject has the right, at the request of the Data Controller, to restrict the data processing instead of correcting or deleting personal and special data, if one of the following is met:

- the Data Subject disputes the accuracy of the personal data, in which case the restriction applies to the period of time that allows the Data Controller to verify the accuracy of the personal data;
- the data processing is illegal and the Data Subject opposes the deletion of the data and instead requests a restriction on their use;
- the Data Controller no longer needs the personal data for the purpose of data processing, but the Data Subject requests them in order to submit, enforce or protect legal claims; obsession
- the Data Subject has objected to the data processing; in this case, the restriction shall apply for the period until it is determined whether the legitimate reasons of the Data Controller take precedence over the legitimate reasons of the data subject.

If the processing is restricted, such personal data may be processed, except for storage, only with the consent of the data subject or for the purpose of bringing, enforcing or protecting legal claims or protecting the rights of another natural or legal person or in the important public interest of the Union or a Member State.

The Data Controller shall inform the Data Subject, at whose request the data processing has been restricted, of the lifting of the data processing restriction in advance.

11.5. Obligation to notify the rectification or erasure of personal data or the restriction of data processing

The Data Controller shall inform all recipients to whom or with whom the personal data have been communicated of the rectification, erasure or restriction of the processing of personal data, unless this proves impossible or requires a disproportionate effort. Upon request, the Data Controller shall inform the Data Subject of these recipients.

11.6. Right to protest

The Data Subject may object to the processing of his or her personal or special data if the processing:

- is necessary for the performance of a task in the public interest or in the exercise of a public authority granted to the Data Controller;
- necessary to enforce the legitimate interests of the Data Controller or a third party;
- based on profiling.

In the event of a data subject's objection, the Data Controller may not further process the personal data, unless it proves that the data processing is justified by compelling legitimate reasons which take precedence over the data subject's interests, rights and freedoms or related to the submission, enforcement or protection of legal claims.

If the processing of personal data is carried out for the purpose of direct business acquisition or related profiling, the Data Subject has the right to object at any time to the processing of personal data concerning him or her for this purpose. If the Data Subject objects to the processing of personal data for the purpose of direct business acquisition, the personal data may no longer be processed for this purpose.

The Data Controller shall, without undue delay, but no later than **within 30 days** of receipt of the request, inform the Data Subject of the action taken on the request for access, rectification, erasure, restriction, protest and data portability. If necessary, taking into account the complexity of the application and the number of applications, this period **may be extended by a further two months**. The Data Controller shall inform the Data Subject of the extension of the deadline, indicating the reasons for the delay, **within 30 days from the receipt of the request**. If the data subject has submitted the request by electronic means, the information shall, as far as possible, be provided by electronic means, unless the data subject requests otherwise.

If the Data Controller fails to take action on the Data Subject's request, it shall inform the Data Subject **without delay, but no later than within one month of receipt of the request, of the reasons for the non-action** and of the Data Subject's right to appeal to a supervisory authority.

Upon the request of the Data Subject, the information, information and action taken on the request shall be provided free of charge. If the Data Subject's request is manifestly unfounded or, in particular due to its repetitive nature, excessive, the Data Controller may charge a reasonable fee or refuse to act on the request, taking into account the administrative costs of providing the requested information or action or taking the requested action. The burden of proving that the request is manifestly unfounded or excessive is on the Data Controller.

12.) Data security

The Data Controller undertakes to ensure the security of the data, to take the technical and organizational measures and to establish the procedural rules that ensure that the recorded, stored and processed data are protected, and to prevent their destruction and unauthorized use. and unauthorized alteration. It also undertakes to call on all third parties to whom the data are transmitted or transferred with the consent of the data subjects to comply with the data security requirement.

The data controller shall ensure that the processed data cannot be accessed, disclosed, transmitted, modified or deleted by unauthorized persons. The data processed may only be accessed by the Data Controller and its authorized employees, persons in an employment relationship with the Data Controller to the extent lawful, and the Data Controller shall not transfer them to a third party who is not entitled to access the data.

The data controller will do everything in its power to ensure that the data is not accidentally damaged or destroyed. The Data Controller imposes the above commitment on the employees participating in the data management activities.

The following data protection solutions are available from the data controller:

- paper-based data carriers are placed in a lockable room, access to them is limited to those who are entitled to them
- the storage facilities of the server park are protected from intrusion, the user accounts of the computers are password protected;

Data processing is secure for privacy impact assessme

13.) Handling and reporting privacy incidents

A data protection incident is any event that involves the unlawful handling or processing of personal data in connection with personal data handled, transmitted, stored or processed by the Data Controller, in particular unauthorized or accidental access, alteration, communication, deletion, loss or destruction and accidental destruction and resulting in injury.

The Data Controller shall, without undue delay, but no later than 72 hours after becoming aware of the data protection incident, notify the NAIH of the data protection incident, unless the Data Controller can demonstrate that the data protection incident is not likely to jeopardize the rights and freedoms of individuals. viewed. If the notification cannot be made within 72 hours, the reason for the delay shall be stated and the required information may be provided in detail without further undue delay. The notification to the NAIH shall contain at least the following information:

- the nature of the data protection incident, the number and category of data subjects and personal data;
- Name and contact details of the data controller;
- the likely consequences of the data protection incident;
- the measures taken or planned to deal with, prevent or remedy the data protection incident.

The Data Controller shall inform the data subjects about the data protection incident via the Data Controller's website within 72 hours after the detection of the data protection incident. The information shall contain at least the information specified in this point.

The Data Controller keeps a record of data protection incidents in order to monitor the measures related to the data protection incident and to inform the data subjects. The register contains the following information:

- the scope of the personal data concerned;
- the range and number of stakeholders;
- the date of the data protection incident;
- the circumstances and effects of the data protection incident;
- Measures taken to deal with the data protection incident.

The data contained in the register shall be kept by the Data Controller **for 5 years from the detection** of the data protection incident.

14.) Enforcement options

14.1. iContrall internal enforcement

The Data Controller makes every effort to process personal data in accordance with the applicable legislation, however, if the Data Subject feels that this has not been complied with, it is possible to write to the e-mail address info@icontrall.com or **2120 Dunakeszi, Eszék utca to a postal address**.

14.2. Enforcement before Naih

If the Data Subject feels that his or her right to the protection of personal data has been violated, he or she may lodge a complaint with the National Data Protection and Information Authority:

Name: **Nemzeti Adatvédelmi és Információs Hatóság**

Headquarters: 1125 Budapest Szilágyi Erzsébet fasor 22/c.

Postal address: 1530 Budapest, Pf.: 5.

Phone number: +36 (1) 391-1400

Fax: +36 (1) 391-1410

Website: <http://naih.hu>

Complaint handling: <http://www.naih.hu/panaszuegyintezes-rendje.html>

14.3. Judicial enforcement

The Data Controller is obliged to prove that the data processing complies with the provisions of the law. The recipient of the data must prove the lawfulness of the data transfer. The court has jurisdiction to hear the case. The action may, at the option of the person concerned, be brought before the court for the place where the person concerned is domiciled or resident.

A party who does not otherwise have legal capacity to sue may also be a party to a lawsuit. The Authority may intervene in the proceedings in order for the person concerned to succeed. If the court grants the request, it obliges the Data Controller to provide the information, to correct, block, delete the data, to annul the decision

iContrAll Ltd. Privacy and privacy policy

made by the automated data processing, to take into account the data subject's right of objection or to release the data requested by the data recipient.

If the court rejects the data recipient's request, the Data Controller shall delete the personal data of the data subject within 3 days from the notification of the judgment. The Data Controller is obliged to delete the data even if the data recipient does not go to court within the specified time limit.

The court may order the publication of its judgment, by publishing the identification data of the Data Controller, if the interests of data protection and the protected rights of a larger number of data subjects so require.

14.4. Compensation and damages

If the Data Controller violates the data subject's right to privacy by illegally handling the data subject's data or violating the data security requirements, the Data Controller may claim damages from the Data Controller. The Data Controller is liable to the data subject for the damage caused by the data processor and the Data Controller is also obliged to pay the data subject the indemnity fee for the personal data violation caused by the data processor. The Data Controller shall be released from the liability for the damage caused and the obligation to pay the damages fee if it proves that the damage or the violation of the personal rights of the data subject was caused by an unavoidable cause outside the scope of data processing.

No damages shall be payable and no damages shall be payable in so far as the damage was caused by the intentional or grossly negligent conduct of the injured party or the breach of the right to privacy.

15. Document data

This document is a self-registered and issued document of the data management of iContrAll Kft.
Version number: 2.0

16. Version tracking

Version	Date	Short description of the change
1.0	2017.11.27.	First version
2.0	2022.03.08.	Service providers refreshed

Date: Dunakeszi, 8th March 2022

Present v2.0. Version No. Data Management and Privacy Policy effective from 8th March 2022