PRIVCY TERMS

Valid from: 2021.04.15

1. Introduction

The Intrain Consulting Limited Liability Company (headquarters: 2143 Kistarcsa, Dr. Tibold József utca 36.; tax number: 28758273-1-13, hereinafter the data controller) as the data controller, acknowledges the content of this legal notice as binding on itself. It undertakes to ensure that all data management and data processing related to its activities meet the requirements set out in this information sheet and the applicable legislation.

The data protection guidelines arising in connection with the data management of the data controller are continuously available at https://intrain.app/privacy_terms.pdf.

The data manager reserves the right to change this information at any time. It places attention-grabbing information on the scope and date of the changes in the application and on the website.

The data manager is committed to protecting the personal data of its users and partners, and considers it of utmost importance to respect the right of informational self-determination of its users and partners. The Data Controller treats personal data confidentially and takes all security, technical and organizational measures that guarantee data security.

Below, the Data Controller describes its data management principles, presents the expectations it has set for itself as a data controller, and adheres to them. Its basic data management principles are in line with the applicable legislation on data protection, and in particular with the following:

- No. 679/2016 General Data Protection Regulation (Regulation)
- CXII of 2011. Act - on the right to self-determination of information and freedom of information (Infotv.);
- CVIII of 2001 Act - on certain issues of electronic commercial services and services related to the information society (Elker's Act);

2. Legal bases during data processing by the Data Controller

In most cases, the Data Controller manages personal data based on a contract. In addition, the fulfillment of your legal obligations also forms the basis of your data management.

3. Scope of personal data, purpose, title, and duration of data management

No	Purpose of data management (Process)	Category	Managed personal data	Legal base	Recipients, categories of recipients	Storage place and methods	Deletion deadline	Data forwarding
	RELATED TO PROVISION OF SERVICE							
1.	**Partner registration and profile creation**	Partners	IP address, e-mail address, password, administrator name, association name, country, city data that can be optionally entered when editing a profile: bank account, deadline for paying the membership fee (day of the month), profile picture, background image	the consent of the person concerned, or the Elker tv. 13/A. (3) of §	-	electronic	until the partner withdraws her consent or deletes her profile or 1 year from the last login = inactivity)	-
2.	**User registration and profile editing**	Users	IP address, e-mail address, password, gender and date of birth for players can optionally be specified when editing a profile: family name, first name, city	the consent of the person concerned, or the Elker tv. 13/A. (3) of §	-	electronic	until the partner withdraws her consent or deletes her profile or 1 year from the last login = inactivity)	-
3.	**Service billing**	Partners	Name, registered office, tax number	Fulfilling the Data Controller's legal obligations	To the authorities specified in the legislation	electronic	Section 169 (2) of the Accounting Act - the cancellation deadline specified in the relevant legislation - 8 years	accountant, invoicing program
4.	**Google OAuth**	Users	Email	Connecting the google login with the registered user by email		electronic	until the partner withdraws her consent or deletes her profile or 1 year from the last login = inactivity)	
5.	**Calculation of adolescence index**	Athletes	mass, height, reach distance	the consent of the person concerned	-	electronic	given that these data are anonymized, they remain in the system	

							for statistical purposes	
6.	**Customer correspondence**	Partners, users	name, e-mail address, IP address, e-mail content, other voluntarily provided personal data	Legitimate interest: fulfilling the contract, servicing user and partner needs	-	electronic	Max 5 years	-
7.	**Complaint handling:** **If you have contacted us with a complaint, data management and the provision of data are essential. If you submit your complaint via the telephone customer service, a record of your complaint will be prepared with the following processed data.** **Investigation of quality complaints, a service that meets the needs of users/partners.**	complainant	name, address, date of complaint, description of the error, claim to be asserted and method of settling the objection	Fulfilling AK's legal obligations	data processors, relevant authorities	electronic	Fogyasztóvédelmi törvény - az adott jogszabályban meghatározott törlési határidő – 5 év	Fogyasztóvédelmi hatóság kérésére
	RELATED TO PROVISION OF SERVICE							
1.	**Making statistics about the use of the application**	application users	e-mail address, IP address	the consent of the person concerned	-	electronic	max 8 years	-

Other data management

We provide information on data management not listed in this information when the data is collected.

We inform our customers that the court, the prosecutor, the investigative authority, the infringement authority, the public administrative authority, the National Data Protection and Freedom of Information Authority, or other bodies based on the authorization of the law, may contact the data controller.

If the authority has specified the exact purpose and scope of the data, the Data Controller will only release personal data to the authorities to the extent and to the extent that is absolutely necessary to achieve the purpose of the request.

4. A személyes adatok tárolásának módja, az adatkezelés biztonsága

The Data Controller's computer systems and other data storage locations are the computer data center rented by the Data Controller (Hetzner Online Gmbh, Industriestr. 25., 91710 Gunzenhausen, Germany).

The Data Controller selects and operates the IT tools used for the management of personal data during the provision of the service in such a way that the managed data:a) az arra feljogosítottak számára hozzáférhető (rendelkezésre állás);

a) its authenticity and authentication are ensured (authenticity of data management);

b) its immutability can be verified (data integrity);

c) be protected against unauthorized access (data confidentiality).

The Data Manager protects the data with appropriate measures, in particular against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction, damage, and inaccessibility resulting from changes in the technology used.

In order to protect the data files managed electronically in its various records, the Data Controller ensures with an appropriate technical solution that the stored data cannot be directly linked and assigned to the data subject, unless permitted by law.

In view of the current state of technology, the Data Controller ensures the protection of the security of data management with technical, organizational and organizational measures that provide a level of protection corresponding to the risks associated with data management.

The Data Controller keeps the following during data management:

a) confidentiality: protect the information so that only those who are authorized to do so can access it;

b) integrity: protects the accuracy and completeness of the information and the method of processing;

c) availability: it ensures that when the authorized user needs it, he can really access the desired information and that the related tools are available.

The Data Controller's IT system and network are both protected against computer-supported fraud, espionage, sabotage, vandalism, fire and flood, as well as computer viruses, computer intrusions and denial-of-service attacks. The operator ensures security with server-level and application-level protection procedures.

We inform users that electronic messages transmitted on the Internet, regardless of the protocol (e-mail, web, ftp, etc.), are vulnerable to network threats that lead to unfair activity, contract disputes, or the disclosure or modification of information. In order to protect against such threats, the data controller takes all necessary precautions. Monitors systems to capture any security discrepancies and provide evidence for any security incidents. In addition, system monitoring also makes it possible to check the effectiveness of the precautions used.

5. The Data Manager's contacts:

Name: Intrain Consulting Korlátolt Felelősségű Társaság

Office: 2143 Kistarcsa, Dr. Tibold József utca 36.

Company registration number: Cg.13-09-207477

Name of the registering court: Fővárosi Törvényszék Cégbírósága

Tax number: 28758273-1-13

Data Protection Officer: Dávid István

E-mail: info@intrain.app

6. Data and contact details of the data processor

Information and contact information of the data processor Data processor (hereinafter: "DP"): the natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller; (Article 4, 8 of the Regulation)

The use of the data processor does not require the prior consent of the data subject, but information is required. Accordingly, we provide the following information.

The data processors are listed below by data management purpose in tabular form for easier transparency:

Data processing activity	DP name, contact	Type
DP related to service provision		
On-line payments	Barion Payment Zrt. 1117 Budapest, Infopark sétány 1. I. ép. 5. em. 5. cjsz: 01-10-048552	regular
DP related to operations		
Könyvelő/bérszámfejtő	SZU-MA PLUSZ Kft. 1213 Budapest, Csalitos út 11. cjsz: 01-09-362376	monthly
Servers, storage	Hetzner Online Gmbh Industriestr. 25., 91710 Gunzenhausen, Germany	regular
Accounting program	NATURASOFT Magyarország Kft. 1113 Budapest, Daróczi út 11. cjsz: 01-09-870298	monthly

The list of data processors is not exhaustive, the Data Controller reserves the right to use additional data processors, the identity of which will be provided individually at the latest at the start of data processing.

7. Information about the data subject's rights

7.1. Right to prior information

The data subject has the right to receive information about the facts and information related to data management before the start of data management.

7.2. The data subject's right of access

The data subject has the right to receive feedback from the Data Controller as to whether his personal data is being processed, and if such data processing is in progress, he is entitled to receive access to the personal data and the related information specified in the Regulation.

7.3. Right to rectification

The data subject is entitled to have the Data Controller correct inaccurate personal data concerning him without undue delay upon request. Taking into account the purpose of data management, the data subject is entitled to request the completion of incomplete personal data, including by means of a supplementary statement.

7.4. The right to erasure ("the right to be forgotten")

The data subject has the right to request that the Data Controller delete the personal data concerning him without undue delay, and the Data Controller is obliged to delete the personal data concerning the data subject without undue delay if one of the reasons specified in the Regulation exists.

7.5. The right to restrict data processing

The data subject is entitled to request that the Data Controller restricts data processing if the conditions specified in the Regulation are met.

7.6. Notification obligation related to the correction or deletion of personal data or the limitation of data management

The Data Controller informs all recipients of all corrections, deletions or data management restrictions to whom or to whom the personal data was disclosed, unless this proves to be impossible or requires a disproportionately large effort. At the request of the data subject, the Data Controller informs about these recipients.

7.7. The right to data portability

Under the conditions set out in the Regulation, the data subject is entitled to receive the personal data relating to him/her provided to a Data Controller in a segmented, widely used, machine-readable format, and is also entitled to forward this data to another Data Controller without being hindered by the the Data Controller to whom the personal data was made available.

7.8. The right to protest

The data subject has the right to object to his personal data at any time for reasons related to his own situation under point e) of Article 6 (1) of the Regulation (the data processing is in the public interest or necessary for the performance of a task carried out in the framework of the exercise of public authority conferred on the Data Controller) or point f) (the data management is necessary to enforce the legitimate interests of the Data Controller or a third party.

7.9. Automated decision-making in individual cases, including profiling

The data subject has the right not to be covered by the scope of a decision based solely on automated data management, including profiling, which would have a legal effect on him or affect him to a similar extent.

7.10. Restrictions

The EU or Member State law applicable to the Data Controller or data processor may limit the provisions of Articles 12-22 through legislative measures. Article and Article 34, as well as Articles 12–22. in accordance with the rights and obligations defined in Article.

7.11. Informing the data subject about the data protection incident

If the data protection incident is likely to involve a high risk for the rights and freedoms of natural persons, the Data Controller shall inform the data subject of the data protection incident without undue delay.

7.12. The right to lodge a complaint with the supervisory authority (right to an official remedy)

The data subject has the right to file a complaint with a supervisory authority - in particular in the Member State of his or her usual place of residence, workplace or the place of the alleged infringement - if, in the opinion of the data subject, the processing of personal data relating to him/her violates the Regulation.

7.13. The right to an effective judicial remedy against the supervisory authority

All natural and legal persons are entitled to an effective judicial remedy against the legally binding decision of the supervisory authority concerning them, or if the supervisory authority does not deal with the complaint, or does not inform the person concerned about the procedural developments related to the submitted complaint or its result within three months.

7.14. The right to an effective judicial remedy against the data controller or data processor

Everyone concerned is entitled to an effective judicial remedy if, in their opinion, their rights under the Regulation have been violated as a result of the processing of their personal data not in accordance with the Regulation.

8. Submission of the data subject's request, actions of the data controller

The data subject may request information about the management of his personal data, as well as request the correction of his personal data or, with the exception of mandatory data processing, its deletion or blocking in the manner indicated at the time of data collection, or via customer service.

The Data Controller shall inform the data subject without undue delay, but in any case within one month of the receipt of the request, of the measures taken as a result of his request to exercise his rights.

If necessary, taking into account the complexity of the application and the number of applications, this deadline can be extended by another two months. The Data Controller shall inform the data subject of the extension of the deadline, indicating the reasons for the delay, within one month of receiving the request.

If the data subject submitted the request electronically, the information must be provided electronically, if possible, unless the data subject requests otherwise.

If the Data Controller does not take measures following the data subject's request, it shall inform the data subject without delay, but at the latest within one month of the receipt of the request, of the reasons for the failure to take action, and of the fact that the data subject may file a complaint with a supervisory authority and exercise his right to judicial redress.

The Data Controller provides information according to Articles 13 and 14 of the Regulation and information about the rights of the data subject (Articles 15-22 and 34 of the Regulation) and measures free of charge. If the data subject's request is clearly unfounded or - especially due to its repetitive nature - excessive, the Data Controller may, taking into account the administrative costs associated with providing the requested information or information or taking the requested measure, refuse to take action based on the request, however, proof of the clearly unfounded or exaggerated nature of the request shall allow the Data Controller is burdened.

If the Data Controller has reasonable doubts about the identity of the natural person who submitted the request, it may request the provision of additional information necessary to confirm the identity of the person concerned.

When exercising the right to data portability, the data subject is entitled to - if this is technically feasible - request the direct transmission of personal data between data controllers.

The Company, as a data controller, provides information about the data it manages, or processed by the processor commissioned by it, its source, the purpose, legal basis, duration of data processing, the name and address of the data processor and its activities related to data processing, as well as, in the case of data transmission, its legal basis and recipient. The data controller shall provide the information in writing as soon as possible after the submission of the request. This information is free of charge if the information requester has not yet submitted a request for information to the data controller regarding the same data set in the current year. In other cases, the Company determines reimbursement.

The Company may not delete the data of the data subject if it is based on the contract, the fulfillment of a legal obligation or the legitimate interest of the Company.

In the case of legitimate interest-based data processing, the data subject has the right to object according to Article 21 of the Regulation, i.e. he can object to the data processing at any time. In this case, the data controller may no longer process the personal data, unless the data controller proves that the data processing is justified by compelling legitimate reasons that take precedence over the interests, rights and freedoms of the data subject, or that are related to the submission, enforcement or defense of legal claims.

The Company compensates for damage caused to others by unlawful handling of the data subject or by breach of data security requirements. The data manager is exempted from responsibility if the damage was caused by an unavoidable cause outside the scope of data management. It does not reimburse the damage to the extent that it resulted from the intentional or grossly negligent behavior of the injured party.

Legal remedies and complaints can be made at the National Data Protection and Freedom of Information Authority:

Nemzeti Adatvédelmi és Információszabadság Hatóság
Office: 1055 Budapest, Falk Miksa utca 9-11.
Address: 1363 Budapest, Pf. 9.
WWW: http://www.naih.hu
Telefon: 06.1.391.1400
Telefax: 06.1.391.1410
E-mail: ugyfelszolgalat@naih.hu

In the event of a violation of their rights, the data subject may also apply to court against the data controller. The court acts out of sequence in the case.

9. Updating information, following legislative changes

The Data Controller continuously revises and updates the Information Sheet in accordance with changes in the legal environment and the authorities' expectations. You can find out more about the current information under https://intrain.app/privacy_policy.pdf.