

DATA HANDLING

1. Data controllers

Name: HRP Europe Ltd.

Address: 1033 Budapest, Huszti út 34.

Representative of the data controller Imre Pál

Name: FixDirect Ltd.

Address: 1033 Budapest, Huszti út 34.

Representative of the data controller András Botzheim

Name: HRP Europe Ltd.

Address: 1033 Budapest, Huszti út 34.

Representative of the data controller Robert Julius Telc

Hereinafter: Data Controllers

Contact details of data controllers regarding data protection: adatvedelem@hrp.hu

This policy is a unilateral commitment of data controllers by Regulation (EU) 2016/679 of the European Parliament and the Council (27 April 2016) and the relevant provisions of the member states.

This policy may be unilaterally amended and/or withdrawn by the data controllers at any time, with the simultaneous notification of the data subjects. The notification enters into effect by its publication on the website or by direct notification of the data subjects, depending on the nature of the change.

1.1 Joint controlling roles and responsibilities

Data controllers inform the data subjects that, according to Article 26 of the GDPR, they are considered joint controllers. In view of this, according to the expectations of the GDPR, the parties agreed with each other on their responsibility for fulfilling the data controller's obligations under the GDPR, as well as their responsibility towards the data subjects as follows:

- HRP Europe Ltd performs the following data processing activities: maintaining contact with its own contracted partners, processing requests and notifications regarding the rights of data subjects related to the GDPR and performing tasks related to data processing incidents.
- FixDirect Ltd performs the following data processing activities: maintaining contact with its own contracted partners.
- HRP Hungary Ltd performs the following data processing activities: maintaining contact with its own contracted partners

1.2 Enforcement of Rights of Data Subjects

Data controllers inform the data subjects that based on Section 3 of Article 26 of the GDPR, data subjects may assert their rights against any controller.

2. A Purposes of data processing

2.1 Management of those registering for events

Registering the data of the data controller's invited customers, contact persons of contracted partners or private individuals delegated by the partner companies, employees of the partner company and invited family members, as well as handling the data of natural persons invited to an open event. Participation in the event is subject to registration and specifying the number of guests arriving together with the registered person.

Processing the data of those registered for events

Legal basis for data processing: Consent

Scope of processed data: Name, company name, position, email address, telephone number, interests, number of adult guests, number of children (under 16) guests, additional information provided by the user

Planned deadline for data processing: Until the withdrawal of the data subject's consent

2.2 Management of data in the case of participants under 16 registering for events

Processing the data of those registered for events

Legal basis for data processing: Consent of the legal representative concerned

Scope of processed data: Name, address, age, email address, telephone number, name of the legal representative, identity card number, signature

Planned deadline for data processing: Until withdrawal, but no later than the last working day of the month of March of the 1st year following the attendance.

2.3 Management of invitees to events

Sending out invitations to events, registering attendance at previous events, and controlling entry to events. Promotion of products distributed by data controllers at events

Legal basis for data processing: Legitimate interest – it is the legitimate interest of the data controllers to invite their partners to events organised by them

Scope of processed data: Name, Company Name, position, email address, telephone number, number of adult guests, number of children (under 16)

Planned deadline for data processing: Until the objection of the person concerned.

2.4 Newsletter service, advertising of new products and service(s), provision of information about products

Requests for new or renewed services, direct marketing or marketing with advertising content, customer satisfaction surveys, invitations to marketing events

Legal basis for data processing: Consent

Scope of processed data: Name, notification address, email address, telephone number, additional information provided by the user

Planned deadline for data processing: Until the withdrawal of the data subject's consent

2.5 Newsletter service, advertising of new products and service(s), provision of information about products

Requests for new or renewed services, direct marketing or marketing with advertising content, customer satisfaction surveys, and invitations to marketing events.

Legal basis for data processing: Legitimate interest—direct business development is the data controller's legitimate interest. The data subject has provided the following data to the data controllers by using any of their services. In this policy, the data controllers inform the data subject of the reclassification of the

data processed in accordance with the activities recorded in 2.1 and 2.2 and use it for direct marketing purposes on the grounds of legitimate interest.

Scope of processed data: Name, notification address, email address, telephone number, additional information provided by the user

Planned deadline for data processing: Until the objection of the person concerned.

2.6 Handing over prizes

The data controller shall have a receipt signed for the prizes upon handing them over.

Legal basis for data processing: Legal obligation

Scope of processed data: Name, company name, signature

Planned deadline for data processing: 8 years (until 31 December of the 8th year)

2.7 Event photos, video documentation

The data controllers make photo and video recordings of the events, which are published on the website, social media pages (Facebook, LinkedIn) and YouTube of the data controllers.

The participant explicitly contributes to the pictures and video recordings of it in the above media after this event.

Legal basis for data processing: Consent

Scope of processed data: Face and body image, video recording

Planned deadline for data processing: Until the withdrawal of the data subject's consent

2.8 Cleaning partner contact data:

The data controller compares the contact details of the contacts delegated to the event by its customers and contracted partners with its own contact database and updates them with the data provided in connection with the event.

Legal basis for data processing: Legitimate interest– keeping contact data up to date is the data controller's legitimate interest.

Scope of processed data: Name, Company Name, position, email address, telephone number

2.9 Travel arrangements for partners

Booking of events, training sessions, travel, accommodation and programme participation organised for the partners of the data controllers.

Legal basis for data processing: Consent

Scope of processed data: Name, address, email address, telephone number, IT log file, ID number, passport number, driver's licence number, date of birth, place of birth

Planned deadline for data processing: Until the withdrawal of the data subject's consent

2.10 Operation of an electronic surveillance system to protect the following:

Operation of an electronic monitoring system to protect the following:

- Security of the data controller's premises
- Protection of the property of the data controller
- Protecting the health and property of the data controller's employees and visitors
- Investigating the circumstances of accidents and crimes that may occur

Legal basis for data processing: Consent and Legitimate interest

Scope of processed data: Face and body image or recording

Planned deadline for data processing: 1 year

2.11 Management of cookies

Identification of users, Cookies typical of webshops are so-called "password-protected session cookies", "shopping cart cookies" and "security cookies", the use of which does not require prior consent from the data subjects.

Legal basis for data processing: Legitimate interest – it is the data controller's legitimate interest to optimise and monitor their services.

Scope of processed data: Unique ID number, dates, times

Planned deadline for data processing:

Last login date: will be deleted after 1 day,

Login data: deleted after 30 days,

login window login data and cookies accepted: deleted after 1 year,

Product comparison data: deleted after 2 years,

Scope of data subjects: Everyone visiting the website.

Potential data controllers entitled to access the data: The data controller does not process personal data through the use of cookies.

Description of the rights of data subjects related to data processing: The data subject has the option to delete cookies in the Tools/Settings menu of their browsers, usually under the settings of the menu item "Privacy".

3. Scope of data subjects

The data controller's invited customers, contact persons of contracted partners or private individuals delegated by the partner companies, employees of the partner company and invited family members.

4. Children

Our products and services are not intended for persons under the age of 16, and we ask that persons under the age of 16 not to provide personal data to the controller. If we become aware that we have collected personal information from a child under the age of 16, we will take steps to delete it as soon as possible.

The exception to this is Section 14.2, where the data controller handles data processing only with the express consent of the legal representative in the case of persons under 16 years of age.

5. Duration of data management:

In case of consent: until the Data Subject withdraws his consent, but for a maximum of 3 years.

In case of legitimate interest: until the Data Subject objects

The data controller uses the recordings stored in the electronic monitoring system in accordance with CXXXIII of 2005 on the rules of personal and property protection and private investigative activities. stored for the period specified in the provisions of the Act (Szvtv.).

The Data Controller applies the following retention periods for recordings made by the electronic monitoring system: Generally 3 days in the evening

In case of damage or suspicion of damage to the assets of the data controller, for the shortest period of time necessary to achieve the goal, if the recordings are used

After the storage period has expired, the recordings are destroyed.

6. Information on the use of a data processor

The data controller transmits the data to the data processor(s) contracted for the performance of the contract.

Categories of recipients: transport companies, IT operators, newsletter system operators, web hosting service providers, web content developer, accounting service providers, the Hungarian Post, security service providers, internet payment service providers, event organising companies, photo and video service companies, notary, lawyer, travel agencies, air lines, hotels and other accommodation providers, activity sites, contracted service partners, contracted reseller partners, contracted suppliers, authorities.

7. Scope of mandatory data

The data controller shall not indicate the data to be filled in separately on each data entry interface, on which entering all data is mandatory. On surfaces where not all data is required, the data controller indicates the mandatory data fields by displaying a "*".

8. Possible consequences of non-provision of data:

If the data subject does not provide their data, they cannot request the services of the data controller.

9. Persons entitled to access the data

The data obtained are collected by the data controller shall not be transferred to third parties, with the exception of data processors indicated in Section 6. Only employees of the controller and designated employees of the processor(s) can know the recorded data.

The recordings obtained and collected by the data controller shall not be transferred to third parties, with the exception of security services and authorities indicated in Section 6. Only employees of the controller and designated employees of the processor(s) can know the recordings.

The managing director, the HR director, the logistics director and the operational director shall have access to the recordings previously recorded by the electronic monitoring system. At their request, the data subject may only access the recordings made exclusively of them in the presence of one of the persons mentioned above. In all cases, you must apply in writing to the data protection manager for access.

In all cases, the data controller shall draw up a report on the fact of sighting the document, which shall be stored by the company for 1 year.

9.1 The images of the electronic surveillance system can be restricted.

The restriction of recordings recorded by the electronic surveillance system can only be implemented in cases where the controller has detected an event that is likely to endanger the objective pursued by the electronic surveillance system.

At the request of the data subject, only the processing of recordings made of them may be restricted. The data subject must apply in writing to the data protection manager for this restriction, indicating its purpose and the expected duration.

The data controller shall draw up a record of every step of the blocking process, which shall be stored by the data controller for 1 year.

10. Processing of data received from third parties

If the user/partner does not provide their own data to the data controller but that of another natural person, it is the user/partner's sole responsibility that the data was provided with the consent, knowledge and appropriate information of this natural person. The data controller is not obliged to examine their existence. The data controller draws the attention of the user/partner to the fact that if the data subject fails to comply with this obligation and therefore enforces a claim against the data controller, the data controller may pass on the executed claim or the amount of the related damage to the user/partner.

11. Rights of data subjects

The data subject may request Information from the data controller regarding the processing of their data,

- as indicated in Section 1.
- They may request the correction of their data,
- they can request information about data management
- request the deletion of their personal data and the restriction of processing,

The data subject may exercise these rights at any time.

The data subject may send this To the data controller at an address indicated in Section 1.

- they can request the transfer of their data to another data controller if the processing is based on a contract or consent, and the organisation processes it in an automated process.
- they withdraw their consent previously given to data processing

The data controller shall arrange or reject this request (stating the reasons) no later than 1 month after the submission of the request – in exceptional cases, within a longer period permitted by law. The data subject shall be informed of the results of the investigation in writing.

11.1 Cost of information

In the first instance, the organisation takes the measures and provides the necessary information **free of charge**.

If the data subject requests the same data, which hasn't changed, twice within a month, the data controller will charge an administrative fee.

- The basis for calculating the administrative is the hourly cost of the current minimum wage as an hourly fee.
- The number of hours worked for the information is calculated at the former hourly rate.
- In addition, in the case of a paper-based information request, the cost of printing the response at cost price and the cost of mailing.

11.2 Refusal of providing information

If the request is clearly **unfounded**, the data controller is not entitled to provide information or the organisation, as the data controller, can prove that the data subject already has the requested information.

In particular, because of its repetitive nature, the request is **excessive**, the organisation may refuse to act on the basis of the request if

- the data subject requests the same data for a third time within a month, exercising their rights.

11.3 Right to object

The data subject shall have the right to object at any time to the processing of their personal data on the basis of a legitimate interest or public authority.

In this case, the organisation shall no longer process the personal data unless they can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

If they establish the well-grounded nature of the legal basis for the objection, they shall terminate the processing of data as soon as possible – including the transfer of data and further data collection. They will notify of the objection all those to whom the data subject has previously transmitted their data.

The processing of the request is free of charge, except for unfounded or excessive requests, for which the data controller may charge a reasonable fee corresponding to their administrative costs. If the data subject does not agree with the decision made by the data controller, they may apply to the court.

12. Disclosure of data

The data controller shall not publish the recordings of the electronic surveillance system.

13. Transfer of data to a third country or to an international organisation

In the case of data transfers to countries outside the EEA, the data controller can transfer the data of the users to the following recipients as data processors with the following conditions.

Addressed to a non-EEA member state	Guarantees of data transfer
Sponsors of events	US Privacy Shield
contracted service partners	US Privacy Shield
contracted suppliers	US Privacy Shield
MailChimp	US Privacy Shield

14. Information on data security measures

The data controller processes the data in a closed system based on the requirements of the Information Security Policy.

The data controller ensures the default and built-in data protection. To this end, the controller applies appropriate technical and organisational measures to:

- Precisely regulate access to data;
- allow access only to persons for whom the data is necessary in order to perform a task with it, and in this case, only to those data that are minimally necessary for the performance of the task;
- carefully select the data processors hired by them and ensure the security of the data with an appropriate data processing contract;
- ensure the integrity, authenticity and protection of the processed data.

The controller applies reasonable physical, technical and organisational security measures to protect the data concerned, in particular against accidental, unauthorised, unlawful destruction, loss, alteration, transfer, use, access or processing. The data controller shall notify the data subject without delay in the event of unauthorised access to or use of personal data which is known and poses a high risk to the data subject.

If the transmission of data is necessary, the data controller shall ensure adequate protection of the transmitted data, for example, by encrypting the data file. The data controller shall be fully responsible for the data processing carried out by third parties.

The data controller also ensures that the data of the data subject are protected against destruction or loss by means of appropriate and regular backups.

15. Legal remedies

Any data subject may also turn to the competent tribunal, the Metropolitan Tribunal in the capital, or initiate an investigation at the National Authority for Data Protection and freedom of information in case of suspected infringement of their rights related to the processing of their personal data.

Chairman: dr. Attila Péterfalvi,
Address: 1374 Budapest, Postbox #603,
Contact: ugyfelszolgalat@naih.hu, +36-1-3911400, www.naih.hu,

Budapest, Nov of 16th, 2020