



# MultiRELOAD

PORT SOLUTIONS FOR SUSTAINABLE MOBILITY

## PRIVACY POLICY

MAY 2023

# TABLE OF CONTENTS

- 1. INTRODUCTION .....3
- 2. PURPOSE AND SCOPE OF THE INFORMATION .....3
- 3. BASIC CONCEPTS .....4
- 4. RIGHTS AND REMEDIES OF THE DATA SUBJECT.....5
- 5. CONTRACT-RELATED DATA MANAGEMENT .....6
- 6. SUPPLIER DATABASE MANAGEMENT .....7
- 7. NEWSLETTER DATABASE MANAGEMENT .....8
- 8. DATA MANAGEMENT DURING EVENT ORGANIZATION .....8
- 9. DATA MANAGEMENT RELATED TO RESEARCH .....9
- 10. DATA MANAGEMENT DURING WEBSITE OPERATION .....9
- 11. MANAGEMENT OF DATA PROTECTION INCIDENTS ..... 10
- 12. DATA ACCESS AND DATA SECURITY MEASURES ..... 11

# 1. Introduction

Hungarian Federation of Danube Ports (hereinafter: HFIP), as data manager and data processor, hereby informs MultiRELOAD Projects' business and professional partners, suppliers, visitors to its website, and all other natural persons whose data it handles (hereinafter collectively: Data Subject(s), that it respects the personal rights of the Data Subjects, and therefore acts on the basis of the provisions of these regulations (hereinafter: Regulations) during its data management.

HFIP declares that it only performs data management based on the provisions of current legislation and handles personal data only in accordance with the legal basis contained in Article 6 of the GDPR.

The version of the Regulations in force is always available in electronic form on the website <https://multireload.eu>. Based on the above, HFIP considers the provisions of the Regulations to be binding on itself and acts in accordance with them during its operation.

## Name of the Data Controller

The name of the data controller	Hungarian Federation of Danube Ports
Abbreviated name	HFIP
Company registration number	07-02-0002817
Headquarter	H-2400 Dunaújváros, Ruhagyári út 5.
Internet contact details	<a href="http://www.hfip.hu">http://www.hfip.hu</a>
Phone number	+36 1 210 9808
E-mail	<a href="mailto:info@hfip.hu">info@hfip.hu</a> ; <a href="mailto:popeiproject@gmail.com">popeiproject@gmail.com</a>

## 2. Purpose and scope of the information

The purpose of this information is to ensure that HFIP complies with the data protection provisions of the current legislation, including in particular (but not exclusively):

- CXII of 2011 on the right to information self-determination and freedom of information. law,
- of Regulation (EU) 2016/679 of the European Parliament and of the Council.

The scope of the Data Management Information covers the business and professional partners of the MultiRELOAD Project, the processing of the personal data of the contracting parties and third parties affected by them.

Clients and partners of individual entrepreneurs, individual companies, shall be considered as natural persons in the application of the Data Management Information.

Temporal effect: These Regulations are effective from **8 May 2023**, until further notice or withdrawal.

HFIP reserves the right to add to or change the data management policy, and thus this Notice, at any time.

### 3. Basic concepts

- **A data controller** is a natural or legal person or an organization without legal personality who, or which - within the framework defined by law or a mandatory legal act of the European Union - independently or together with others determines the purpose of data management, data management (including the used device) makes and implements relevant decisions, or has them implemented by the data processor;
- **A data file** is the totality of the data managed in a register;
- **Data management**, regardless of the procedure used, is any operation performed on the data, or the set of operations, including, in particular, collection, recording, recording, organization, storage, change, use, query, transmission, disclosure, coordination or connection, blocking, deletion and destruction, as well as preventing further use of the data, taking photographs, audio or video recordings, and recording physical characteristics suitable for identifying the person (e.g. fingerprint or palm print, DNA sample, iris image);
- **Data transmission** is making the data available to a specific third party;
- **Data deletion** is the rendering of data unrecognizable in such a way that their recovery is no longer possible;
- **Data destruction** is the complete physical destruction of the data carrier containing the data;
- **A data processor** is a natural or legal person or an unincorporated organization who, within the framework and conditions defined by law or a mandatory legal act of the European Union, processes personal data on behalf of or at the direction of the data controller;
- A natural person identified or identifiable on the basis of any information concerned ;
- **Consent is** a voluntary, definite and clear declaration of the Data Subject's will based on adequate information, with which the Data Subject indicates by means of a statement or other behavior that clearly expresses his will that he gives his consent to the processing of his personal data;
- **Personal data** is any information about the Data Subject;
- **Third party is** a natural or legal person, or an organization without legal personality, who is or is not the same as the Data Subject, the data manager, the data processor or the persons who, under the direct control of the data manager or data processor, carry out operations aimed at processing personal data.

## 4. Rights and remedies of the Data Subject

The Data Subject can apply to HFIP:

- prior to the start of data management, information on all facts related to data management,
- providing your personal data and information related to their management,
- correcting or supplementing your personal data,
- limiting the processing of your personal data,
- deletion of your personal data.

At the Data Subject's request, HFIP must provide the Data Subject with information about the Data Subject's personal data, their source, the purpose, legal basis, duration of data processing, the name and address of the data processor and its activities related to data processing, and - in the case of forwarding the Data Subject's personal data - the legal basis for data transmission and recipient.

The Data Subject can request in writing to change any of his personal data (for example, he can change his e-mail address at any time) through the contact information of HFIP. HFIP will comply with the request for modification as soon as possible, but within 30 days at the most, of which it will inform the Data Subject via one of the contact details provided.

The Data Subject may at any time, in writing, request the deletion of his/her personal data managed by HFIP, via HFIP's contact details. We would like to inform you that if the HFIP cannot delete the personal data it manages due to a legal obligation, your request for data deletion will be rejected in accordance with the applicable legal regulations. If there are no legal obstacles to the deletion of your personal data by HFIP, HFIP will grant its request for data deletion, and your personal data will be permanently deleted within 30 days of receipt of the request by HFIP, of which you will be notified in writing.

The Data Subject can request in writing that his personal data be blocked by the HFIP via the HFIP's contact information. The blocking lasts as long as the specified reason makes it necessary to block the data. The Data Subject may request the blocking of the data, for example, if he believes that some of his personal data has been handled illegally by HFIP, but it is necessary for the sake of official or judicial proceedings initiated by the Data Subject that his personal data is not deleted. In this case, HFIP stores the personal data (or the document containing it) until the authority or the court requests it, after which it deletes the data.

Through the HFIP's contact information, any Data Subject has the right to object in writing to the handling of his personal data, if he considers that his personal data would be forwarded or used by the HFIP for a purpose other than the purpose specified in this Data Management Policy, in the absence of prior consent. Thus, for example, any Data Subject may object to HFIP using their personal data for the purpose of direct business acquisition or direct marketing without their consent. The Data Subject may object to data processing even if the data processing by HFIP is necessary to assert the legitimate interests of HFIP, with the exception of data processing based on legal authorization.

**HFIP draws the attention of the Data Subjects that the Data Subjects can exercise their rights by sending a request to the e-mail address [info@hfip.hu](mailto:info@hfip.hu) or through other contact details of HFIP (given in point 1).**

### Submitting a complaint to the supervisory authority

National Data Protection and Freedom of Information Authority

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

Phone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

Web: <http://www.naih.hu>

e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

### Initiation of court proceedings (civil suit).

If you are violated in connection with the exercise of your Data Subject rights or during the processing of your personal data, you may initiate a civil lawsuit against HFIP. The adjudication of the lawsuit falls within the jurisdiction of the court. The procedure can be initiated before the court of the Data Subject's place of residence or residence. The court acts out of sequence in the case. If a violation is established, you can claim compensation and compensation, and the court can oblige the Office to fulfill the rights of the Data Subject.

You can find more information and the contact details of the courts at the following link: <http://birosag.hu/torvenyszekek>

## 5. Contract-related data management

### Scope of managed data and purpose of data management

Personal data	Purpose of data management
Name	establishing and maintaining contact with contractual partners, suppliers, consultants, professional partners, investors, in the case of a site purchase, the property owners or the natural person designated by them, and customers; exercising the rights and obligations arising from the contract
E-mail address	
Phone number	
Post	
Title	

### Legal basis for data management

HFIP collects and processes contact data based on its legitimate interests. HFIP has considered the impact of the contact data on the Data Subjects and determined that this data management does not result in disproportionate and unnecessary restrictions on the interests, fundamental rights and freedom of the Data Subjects.

Data processing is considered lawful even if data processing is necessary to take steps at the Data Subject's request prior to the conclusion of the contract.

Personal data may be transferred for data processing to postal and courier service providers for the purpose of mailing and delivery.

**Duration of data management**

If they are not included in the contract, HFIP will process the contact data for as long as it is absolutely necessary for the fulfillment of the contract, but no more than 5 years from the termination of the contract, if they are part of the contract, for 8 years after the termination of the contract.

## 6. Supplier database management

**Scope of managed data and purpose of data management**

Personal data	Purpose of data management
Name	The name of the supplier partners' contact persons, which is necessary for the identification of natural persons. The management of personal data is necessary for contacting and maintaining contact.
Phone number	The management of the telephone number as contact information serves the purpose of contacting and maintaining contact.
E-mail address	The management of the e-mail address as contact information serves the purpose of contacting and maintaining contact.
Post	Necessary for mediating suppliers to investors.

**Legal basis for data management**

The legal basis for processing personal data processed in connection with the operation of the supplier database is the consent of the person designated for contact.

**Duration of data management**

The personal data contained in the supplier database is managed by HFIP until the Data Subject's consent is revoked. The Data Subject may delete the personal data contained in the supplier database at any time, and at the same time, the Data Subject may revoke the consent to the processing of the provided personal data at any time.

## 7. Newsletter database management

### Scope of managed data and purpose of data management

Personal data	Purpose of data management
Name	The name of contact persons of the stakeholders and consortium partners, which is necessary for the identification of natural persons. The management of personal data is necessary for contacting and sharing news about the project.
E-mail address	The management of the e-mail address as contact information serves the purpose of contacting and sharing news about the project.
Name of organization	Necessary to identify the partner / stakeholder of the project.

### Legal basis for data management

The legal basis for processing personal data is the Data Subject's consent.

### Duration of data management

The personal data contained in the newsletter database and is managed by HFIP until the Data Subject's consent is revoked. The Data Subject may delete the personal data contained in the newsletter database at any time by unsubscribing the newsletter or by sending a request to the e-mail address info@hfip.hu or through other contact details of HFIP (given in point 1).

## 8. Data management during event organization

### Scope of managed data and purpose of data management

HFIP manages the following Personal data about the presenters and participants of the events it organizes: name, e-mail address, position, telephone number, name of the organization/business it represents or is associated with, biographical data of the presenters, image of the Data Subject (photograph, video recording)

The specific purpose of data management is to identify applicants for training and events, maintain contact with the Data Subject, provide regular information, perform the ordered service and prepare the necessary records. In addition, data processing may take place for the purpose of ensuring legal compliance, i.e. if data processing is necessary to fulfill a legal obligation relating to the Office.

### Legal basis for data management

The legal basis for processing personal data is the Data Subject's consent.



### **Duration of data management**

HFIP processes the personal data provided during registration for the events until the consent of the Data Subject is revoked. The Data Subject may withdraw the prior application for the events and, at the same time, the consent to the processing of the personal data provided, at any time, and may initiate the deletion of the personal data.

## 9. Data management related to research

### **Scope of managed data and purpose of data management**

After filling in the questionnaires, the data provided during the research are stored and used in an anonymized manner, separated from the personal data.

HFIP handles the personal data provided to it in connection with research activities exclusively for the purpose of facilitating research activities and is entitled to forward them to third parties only with the Data Subject's consent.

### **Legal basis for data management**

The legal basis for processing the personal data of those who fill in ad hoc questionnaires is the voluntarily given consent of the Data Subjects.

### **Duration of data management**

Personal data provided during the filling out of questionnaires or collected through technical solutions will be processed for a maximum of 60 days, unless otherwise provided before the questionnaire was filled out. The data provided during the survey is processed by removing the personal information from the database, the database copy containing the personal data is deleted within the above deadline.

## 10. Data management during website operation

While browsing MultiRELOAD website, technical information is recorded (for example in the form of log files, which contain the user's IP address, the time, the URL of the page visited), which cannot be used for personal identification, but serves statistical purposes.

When visiting MultiRELOAD website, the system places a cookie on the hard drive of the visitor's computer, provided that this option is enabled in the visitor's browser. The visitor can set the browser used to access the Internet to receive a notification if the website wants to place a cookie on his computer and can also prohibit the sending of cookies at any time. Cookies are not suitable for identifying the user and are active during the session.

# 11. Management of data protection incidents

## The concept of a data breach

A data protection incident is a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise handled.

A data protection incident is, for example, the loss of an office mobile phone or a data storage device, the proper storage of documents containing personal data in a manner not specified in the Document Management Regulations (e.g. salary slips thrown in the trash); transmission of personal data on a non-secure channel, attacks against various servers, website hacking.

## Management of data protection incidents

HFIP is responsible for preventing and handling data protection incidents and complying with the relevant legal regulations.

HFIP logs accesses and access attempts on the IT systems and analyzes them as necessary.

If persons entitled to control on behalf of HFIP notice a data protection incident during the performance of their duties, they must immediately notify the president of HFIP.

When a data protection incident is reported, HFIP immediately examines the report, identifies the incident, and decides whether it is a real incident or a false alarm. It must be examined and determined:

- the time and place of the incident,
- description of the incident, circumstances, effects,
- the scope and number of data compromised during the incident,
- the range of persons affected by the compromised data,
- a description of the measures taken to prevent the incident,
- a description of the measures taken to prevent, eliminate and reduce the damage.

In the event of a data protection incident, HFIP accurately identifies the affected systems, persons, and data, and separates and ensures the collection and preservation of evidence supporting the occurrence of the incident. After that, HFIP will begin to repair the damage and restore legal operations.

## Registration of data protection incidents

HFIP keeps a record of data protection incidents, which includes:

- the scope of personal data of the Data Subject,
- the range and number of persons affected by the data protection incident,
- the date of the data protection incident,
- the circumstances and effects of the data protection incident,
- the measures taken to remedy the data protection incident,
- other data specified in the law that prescribes data management.

HFIP will keep data on data protection incidents in the register for 5 years.

## 12. Data access and data security measures

### Data access and data transfer

Employees of the Office can access the personal data provided by the Data Subject based on the relevant authorization, in order to perform their duties. Thus, for example, during the organization and conduct of events, the persons involved in event organization, in addition to the appropriate data protection measures.

HFIP only in exceptional cases transfers the Data Subject's personal data to other state bodies or market participants.

- based on contractual obligations;
- in the event that the Office organizes an event with the participation of another state body or market participant, it is necessary for the organization of the event and the travel of the persons participating in the event in connection with the event.

### Data security measures

HFIP stores the personal data provided by the Data Subject on devices under its supervision. In order to protect the Data Subject's personal data, HFIP applies a number of technical and organizational security measures in connection with data storage and processing, which are designed to prevent access to data by unauthorized persons.

HFIP implements the protection of the personal data it manages with both software and hardware tools, as well as modern IT methods, high-level encryption and protection.

HFIP imposes an obligation of confidentiality on the handling of personal data for those employed by it, which is signed by the Data Subject in the form of a confidentiality statement upon appointment or upon conclusion of the employment contract.

HFIP takes all measures expected of it to keep the data safe, but assumes no responsibility for the damage, destruction or falling into unauthorized hands of the data in the event of a technical error, natural disaster, terror or crime, and cannot guarantee the complete security of personal data due to security and technical in case of illegal intrusion into the protection system.