

## DATA MANAGEMENT INFORMATION FOR MARKETING COMMUNICATIONS AND EVENTS, AS WELL AS FOR WEBSITE VISITS

HT Division Private Limited Company (hereinafter: Data Manager) provides the following information to the affected persons related to personalized marketing communication, participation in events and the use of website:

Name of Data Manager: HT Division Zártkörűen Működő Részvénytársaság  
Registry No of Data Manager: 01-10-049780  
Seat of Data Manager: 1068 Budapest, Városligeti fasor 38.  
E-contact to Data Manager: [eva.elias@htdivision.com](mailto:eva.elias@htdivision.com)  
Website of Data Manager: HTDIVISION.COM  
Representative of Data Manager: Suat Gökhan Karakus CEO

### I. DATA MANAGERMENTS

#### 1.) Data Management related to Marketing communication (newsletter)

Purpose of Data Management: Establishing effective marketing communication, sending personalized messages to the person concerned based on the behaviour shown on the Data Manager's interfaces.

Claim of Data Management: Your consent (as per EU decree 2016/679, article 6, point a).

Scope of processed data:

Processed data	Purpose of data management
full name	identification of user
e-mail address	personalized communication

Duration of data management: until revoke of consent.

Possible consequences of a failure of supplying of data: The affected person will not get personalized service nor promotions from the Data Manager.

#### 2.) Data management related to participation in events

Purpose of data management: The effective service of the people at events, the documentation of events, the advertising of events on the online platforms of the Data Manager.

Claim of Data Management: Your consent (as per EU decree 2016/679, article 6, point a), which also covers the unrestricted use of photographs and video recordings of the affected person by the Data Manager.

Scope of processed data:

Processed data	Purpose of data management
Name of event	Granting access on the proper event day to the event
full name	identification of user
e-mail address	personalized communication
Photographs and video recordings	Documentation and advertising of the event

Duration of data management: until revoke of consent.

Possible consequences of a failure of supplying of data: The documentation and advertising of the event will not be possible.

### 3.) Cookie policy

Purpose of Data Management: The effective and easy to use handle of Data Manager's webpage.

Claim of Data Management: Your consent (as per EU decree 2016/679, article 6, point a).

Scope of processed data:

<b>Processed data</b>	<b>Purpose of data management</b>
Information related to the use of the website (time, duration of visit, subsequent review of the exhibition, pages viewed, clicks through the pages, use of the search engine)	To enable the user to see relevant information.
Technical information (IP address, cookie identifier, browser type, device type, Google, Facebook identifiers, source page)	To enable the user to see relevant information and personalized offers.
The Data Manager may use the data for statistical purposes. The use of the data in a statistically aggregated form may not include the name of the concerned user or other identifiable information in any form	
Technically recorded data are the data of the User's logged-in computer, which are generated during the use of the service and which are logged by the data management system as an automatic result of technical processes (e.g. IP address, session ID). These data cannot be combined with User's other personal data - except in cases made mandatory by law.	The log files that are automatically and technically recorded during the operation of the system are stored in the system for a reasonable period of time in terms of ensuring the operation of the system.

Duration of data management: until revoke of consent.

Possible consequences of a failure of supplying of data: The affected person will not get relevant information from the Data Manager.

## II. DATA PROCESSING

In accordance with the governing legislation, the Data Manager is entitled to use a data processor for the purpose of certain technical operations or for the provision of the service. The data processor is only entitled to execute the instructions and decisions of the Data Manager.

The Data Manager uses the following data processors:

Company name and seat of data processor	The scope and purpose of the processing	Categories of personal data	Place of processing (and storage) e.g.: country/state	Claim of the handover of personal data
	<i>E.g. security service</i>	<i>E.g. identification data</i>	<i>Hungary</i>	<i>Referral to the agreement between Data Manager and data processor</i>

### III. RIGHTS ENTITLED TO THE PERSON IN CONCERN

The person in concern can request information about the management of his/her personal data; and can furthermore request the correction of his/her personal data; deletion of his/her data at the e-mail address [eva.elias@htdivision.com](mailto:eva.elias@htdivision.com); the limitation of data management; and is entitled to data portability and legal remedies. If you have a complaint, you can apply to the Hungarian National Authority for Data Protection and Freedom of Information or – according to your choice – to a court in Hungary. In court proceedings, the tribunal has jurisdiction.

#### 1. Information and access to personal data

The person in concern has the right to get to know his/her personal data stored by the Data Manager and the information related to their management; check what data the Data Manager keeps about him/her, and the person is also entitled to access the personal data. The person in concern must submit his/her request for access to the data in writing (by e-mail or post) to the Data Manager. The Data Manager provides the information to the person in concern in a widely used electronic format, unless the person in concern requests it in writing, on paper. The Data Manager does not provide verbal information when exercising access over the phone.

In case of exercising the right of access, the information covers the following:

- definition of the scope of processed data, purpose, time and legal basis of data processing with regard to the scope of processed data,
- data transmission: to whom the data has been transmitted, or will be transmitted in the future,
- designation of data source.

The Data Manager provides the person in concern with a copy of the personal data (in person at the customer service) free of charge for the first time. For additional copies requested by the Person in concern, the Data Manager may charge a reasonable fee based on administrative costs. If the Person in concern requests a copy electronically, the Data Manager will provide the person in concern with the information by e-mail in a widely used electronic format.

After receiving the information, if the Person in concern does not agree with the data management and the pertinence of the processed data, he may request the correction, addition, deletion, restriction of processing of his/her personal data, and may object to the processing of such personal data.

## **2. The right to correct and complete processed personal data**

At the Person in concern's written request, the Data Manager shall, without undue delay, correct inaccurate personal data indicated by the person in concern in writing or in person at one of the Data Manager's stores, or supplement the incomplete data with the content specified by the Person in concern. The Data Manager informs all recipients of the correction or addition to whom the personal data has been communicated, unless this proves to be impossible or requires a disproportionately large amount of effort. The Data Manager will provide information about data of these recipients upon written request of the Person in concern .

## **3. Right to restriction of data management**

The Person in concern may, by means of a written request, ask the Data Manager to restrict the processing of his/her data, if

- the Person in concern disputes the accuracy of the personal data, in this case the restriction applies to the period that allows the Data Manager to check the accuracy of the personal data,
- the data management is illegal and the Person in concern opposes the deletion of the data and instead requests the restriction of their use,
- the Data Manager no longer needs the personal data for the purpose of data management, but the Person in concern requires them to submit, enforce or defend legal claims,
- the Person in concern objects to data processing: in this case, the restriction applies to the period until it is determined whether the Data Manager's legitimate reasons take precedence over the Person in concern's legitimate reasons.

If the Person in concern's objection is well-founded, the data will be restricted by the Data Manager, i.e. only storing as data management can be carried out as long as

- the Person in concern consents to data management;
- processing of personal data is necessary to assert legal claims;
- it becomes necessary to manage personal data in order to protect the rights of other natural or legal entities; or
- legislation mandates data management in the interest of the public.

If the restriction of data management has been requested by the Person in concern, the Data Manager will inform the Person in concern in advance about the lifting of the restriction.

## **4. Right to deletion (Oblivion).**

At the request of the Person in concern, the Data Manager shall delete the personal data concerning the affected person without undue delay if one of the specified reasons exists:

- the personal data are no longer needed for the purpose for which they were collected or otherwise managed by the Data Manager;
- the Person in concern withdraws the consent that forms the basis of the data management, and there is no other legal basis for the data management;
- the Person in concern objects to the data processing for reasons related to his/her own situation, and there is no legitimate reason for the data processing,
- the Person in concern objects to the processing of his/her personal data for the purpose of direct business acquisition, including profiling, if it is related to direct business acquisition,
- personal data is handled illegally by the Data Manager;
- the collection of personal data took place in connection with the offering of information-society related services offered directly to children.

The Person in concern may not exercise his/her right to deletion or oblivion if data management is necessary

- for the purpose of exercising the right to freedom of expression and information;
- on the basis of 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, if the exercise of the right to deletion would make this data management impossible or seriously endanger it; or
- to submit, enforce and defend legal claims.

### **5. Right to data portability**

Data portability makes it possible for the Person in concern to acquire and further use the "own" data provided by the Person in concern in the Data Manager's system, for his own purposes and through various service providers determined by him/her. In all cases, the authorization is limited to the data provided by the Person in concern, there is no possibility of portability of other data. (e.g. statistics, etc.)

Personal data of the Person in concern that can be found in the Data Management system (e.g. when subscribing to the newsletter):

- will be given to the Person in concern in a segmented, widely used, machine-readable format,
- Person in concern is entitled to transfer them to another data manager,
- Person in concern can request the direct transfer of data to other data manager - if this is technically feasible in the Data Manager's system.

The Data Manager fulfils the request for data portability only on the basis of a request written by e-mail or post. In order to fulfill the request, it is necessary for the Data Manager to make sure that the person who is entitled to use this right is really the Person in concern. For this, it is necessary for the Person in concern to appear in person at the Data Manager's headquarters after the notification, in order for the Data Manager to be able to identify the requesting Person in concern using the data in its system. Within the scope of this right, the Person in concern may request the portability of the data that he/she has provided to the Data Manager. Exercising the right does not automatically result in the data being deleted from the Data Manager's systems, therefore the Person in concern will be registered in the Data Manager's systems even after exercising this right, unless he/she does not request the deletion of his/her data.

### **6. Objection to the handling of personal data**

The Person in concern may object to the processing of his/her personal data by means of a statement addressed to the Data Manager, if the legal basis for data processing is

- Public interest according to Article 6, paragraph (1) point f) of the GDPR., or
- legitimate interest according to Article 6, paragraph (1) point f) of the GDPR.

In the case of exercising the right to object, the Data Manager may no longer process the personal data, unless the Data Manager proves that the data processing is justified by compelling legitimate reasons that take precedence over the interests, rights and freedoms of the Person in concern, or that are in connection with the presentation, enforcement or defense of legal claims. In connection with the determination that the data processing is justified by compelling legitimate reasons, the Data Manager's executive decides. It informs the Person in concern of its position in this regard in an opinion.

The Person in concern can object in writing (by e-mail or by post).

## **IV. DEADLINE OF FULFILLMENT OF REQUEST, PROCEDURE RULES**

Data Manager without undue delay, but in any case informs the Person in concern about the measures taken within one month from the receipt of any request pursuant to point III. 1-6. If necessary, taking into account the complexity of the request and the number of requests, this deadline can be extended by another two months, but in this case Data Manager will inform the Person in concern within one month of receiving the request, indicating the reasons for the delay as well as that the Person in concern may submit a complaint to a supervisory authority, and can exercise his right to legal redress.

If the Person in concern's request is clearly unfounded or excessive (especially considering the repetitive nature), the Data Manager may charge a reasonable fee for fulfilling the request or refuse to take action based on the request. The Data Manager is responsible for proving this.

If the Person in concern submitted the request electronically, the Data Manager will provide the information electronically, unless otherwise requested by the Person in concern.

The Data Manager informs all such recipients of all corrections, deletions or data management restrictions made by it, to whom or to which the personal data was communicated, unless this proves to be impossible or requires a disproportionately large effort. The Data Manager informs the person in concern upon his / her request about these recipients.

#### **IV. ENFORCEMENT OPTIONS**

The Person in concern may exercise his/her rights against the Data Manager in a written request sent by e-mail or post.

The rights of the Person in concern cannot be asserted if the Data Manager proves that it is not in a position to identify the Person in concern. If the Data Manager has doubts about the identity of the natural person who submitted the request, it can request the provision of additional information necessary to confirm the identity of the requester.

Based on the Act of Information, the Decree and the Civil Code (Act V. of 2013) the Person in concern

- may contact the National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/c.; [www.naih.hu](http://www.naih.hu)) or
- may enforce his / her rights in court.

#### **V. COMPENSATION AND CONCESSION**

Any person who has suffered material or non-material damage as a result of a violation of the Decree is entitled to compensation from the Data Manager or the data processor for the damage suffered. The data processor is only liable for damages caused by data processing if it has not complied with the obligations specified in the law, which are specifically imposed on data processors, or if it has ignored or acted contrary to the lawful instructions of the Data Manager. The Data Manager or the data processor is exempted from liability if it proves that it is not in any way responsible for the event causing the damage.

#### **VI. HANDLING OF DATA PROTECTION INCIDENTS**

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. The Data Manager keeps a register for the purpose of checking the measures related to the data protection incident, informing the supervisory authority, and informing the Person in concern, which includes the range of personal data affected by the incident, the range and number of the affected parties, the date, circumstances, effects of the incident, and the measures taken to prevent it. In the event of an incident - unless it involves a risk to the rights and freedoms of natural persons - Data Manager shall inform the

Person in concern and the supervisory authority of the data protection incident without undue delay, but within 72 hours at most.

## **VII. PROCEDURE FOR HANDLING BACKUP**

As part of its duties related to IT protection, the Data Manager ensures in particular measures to ensure the possibility of restoring data files, including regular backups and the separated, safe handling of copies (backup).

Accordingly, Data Processor - in order to prevent the loss of electronically stored data - backs up the data of its database containing personal data regularly, three times a day, on a separate data carrier.

Backups made from the website server are stored at: DotRoll Kft. backup server

Duration of storage of backups: 5 years

The order of deleting backups: individual deletions can be tracked in an anonymized register, and automatic deletions take place based on settings.

Access to the backup: Access to the backup is limited, only authorized persons can access it. The data can only be accessed after proper personal identification (at least username and password).

## **VIII. OTHER PROVISIONS**

The Data Manager reserves the right to unilaterally modify this Data Management Information. To the person in concern the amendments shall enter into force on the date specified in the notification, unless the Amendment is objected to in writing.

If the Person in concern provided third-party data to use the service and caused damage, the Data Manager is entitled to enforce compensation against the Person in concern.

The Data Manager does not check the personal data provided to him. The person providing the data is solely responsible for the adequacy of the data provided. When providing the data, the Applicant also takes responsibility for the fact that it has the appropriate legal basis for providing the personal data of the contact person and that it has provided his / her employee with the information required by the Decree before transferring his / her data to the Data Manager.

### **Contact details of the Data Protection Contact**

Name: Éva Élias

Phone number: +36706283907

Email: eva.elias@htdivision.com

Date of entry into force of this Data Management Notice: January 2021 \*\*.

Available for download at [www.htdivision.com](http://www.htdivision.com)

HT Division Zrt.