HAPPY KIDS INTERNATIONAL KINDERGARTEN AND NURSERY

DATA PROTECTION/GDPR POLICY 2021

DATA CONTROLLER: HETEDHÉT ORSZÁG ALAPÍTVÁNY

1124 BUDAPEST, FODOR UTCA 36.

TEL: +36-1-3562440

E-MAIL: INFO@HAPPYKIDS.HU

1. Purpose of the policy

The purpose of this Privacy Policy is to set out the principles and procedures of data protection and data management of Hetedhét Ország Alapítvány:

Address: 1124 Budapest, Fodor utca 36.

Tax No: 18101773-1-43

Tel. No: +36-1-356-2440

E-mail: info@happykids.hu

Representative: Peter Frank Jones

as founder and operator of Happy Kids International Kindergarten and Nursery Budapest (hereafter named as „Institution") as a data controller; make them accessible and transparent, and thus comply with the requirements of the regulations of the European Parliament and Council (EU) 2016/679. (GDPR), ie. the EU General Data Protection Regulation.

The policy is explicitly governed by this general EU regulation, its rules are to be interpreted in accordance with the EU GDPR Regulation and all issues not affected directly by this policy are governed by the EU General Data Protection Regulation.

The purpose of the policy is to regulate the personal data management within the activities of the institution; more precisely what kind of data, in what terms, for what purpose, what scope and manner are managed and controlled, how does the

company ensure the security and storage of the managed and controlled data, to who, how and on what basis does it sends the managed and controlled data to any third parties, or make them recognizable by any parties, and how it destroys or makes them unrecognizable.

2. The controlled personal data

As data controller, the institution treats the following personal data that are necessary for its business operations, the full representation of its clients' interests and for compliance with legal requirements:

- Name
- Birth name
- Place and date of birth
- Telephone / electronic contact data
- Address
- Place of residence + residency card (both child+parents)
- Copy birth certificate (child)
- Medical and vaccination records (child)
- Social security number (child)
- Copy of passport/ local ID card (both child+parents)

3. The purpose of data management

The purpose of the data management is primarily to manage and safeguard the data of both children and their parents as the business partners of the institution; to officially keep in touch with them and to provide them with all services they require as clients. This also applies to the data management of the employees of the company, to the necessary extent covering duties of the company as requested by an employer.

The additional purposes of the data management is the successful fulfilment of the contractual agreement between the client and the institution. In doing so, the institution as a data controller manages only the necessary data required by the laws and by the general business and economic activities and rules in Hungary.

In terms of data handling, collecting, management and storage of data, the following laws apply (among others) for the institution as a data controller. The data mentioned above are specifically handled, stored or transferred in accordance with the provisions of these laws and other related legislation

- The Act C. of 2000. on Accounting
- The Act V. of 2006. on company publicity, the court procedures of the company register and the liquidation procedure
- The Act CL. of 2017. on Taxation
- The Act V. of 2013. on the Civil Code
- The Act I. of 2012. on Labour Law
- The Act CXII. of 2011. on information self-determination and freedom of information

The company as a data controller does not process data, does not perform profiling activities, and does not handle special and sensitive data.

The managed data will only be transferred to third parties if the customer explicitly requests it; or the customer is informed about the transfer of data and has given consent; furthermore for the purpose of accounting obligations; or if the data transfer is required by law or public authority through an official decision.

4. The legality of the data management

The institution as data controller manages the personal data of the subjects only in the case of the following:

4.1. The subject gave consent explicitly and in writing to the management of his or her personal data, necessary to meet contractual purposes. These are primarily the fulfilment of the services provided by the company in contractual relations with the clients.

4.2. The data management is necessary to perform the legal obligations for the data controller.

4.3. The data management is necessary to enforce the legitimate interests of the data controller or a third party, unless the interests or fundamental freedoms of the

data subject have priority over those interests and require the protection of their personal data, particularly if the subject is a child.

The purpose of the data management is to enforce the legitimate interests of the institution itself and, where applicable, of a third party. In such special case the management of data is solely based on the legitimate interest of the party, such as settlement dispute, other litigation, and possible official order of the authorities.

In such cases, the data are collected and handled only to the extent strictly necessary to deal with the case of legitimate interests; only the data that has been legitimately handled or is required by third parties (eg. from a court or authority) could be used, and the data management extends to the scope of the actual case.

In these cases, only the exclusively necessary data could be managed for the enforcement of the legitimate interests, solely for the scope of the case.

In order to guarantee the data management's limitations of these cases, the company only manages the personal data related to and in the scope of the case and within the limits prescribed by the law. After the settlement of the case of the legitimate interests, the affected and used personal data will be immediately destroyed.

5. The rights of the subjects of data management

The rights of data subjects and clients are explicitly covered by the regulation of the European Parliament and Council (EU) 2016/679. (GDPR), the rules formulated therein shall govern for the data controller.

Briefly, for information purposes, these are the following:

- The subject is entitled, if the data management is based solely on his / her consent and the data management is therefore not the subject of any statutory obligation, to withdraw his / her consent, after which the data controller immediately destroys the stored data of the affected subject.

- The subject has the right to know the exact data managed and collected by the data controller, which directly affects him / her In the case of such written or verbal request, the company prepares a simplified and understandable summary of the managed data of the affected subject.

- The subject may at any time ask for correction and clarification of his / her data.
- The subject is entitled to request from the data controller to forward the data provided by the subject to any third party given by the data subject.
- The subject may ask the data controller to discard and destroy any of his / her data.
- The subject is entitled to view the privacy policy of the institution as a data controller at any time.

6. Duration, deletion, transfer and storage of the managed data

The data controller actively manages the data primarily through the contractual relationship between the institution as data controller and the client. Following the closure of an active contractual relationship, the institution as a data controller stores the data until the expiry of the general limitation period, which expires on the 5th year after the date of the contract concluded by the parties. If the contractual partner is a legal person, the data necessary for the official contact will be destroyed by the data controller as the contractual relationship is terminated. An exception to this rule is if the termination of the contractual relationship is caused by a dispute, in which case the rules in point 4 will be applied.

The data controller inform the subject that the data controller could transfer his / her personal data at the explicit request of the subject.

In addition, the data controller transfers the data to the accounting company or accountant, with which it has contractual relations in order to fulfil the company's accounting obligations:

KB Audit Kft.

1085 Budapest, Horánszky utca 10.

The data controller shall only transfer data to an official authority if there is an official request or the law prescribes it.

The managed personal data is stored by the data controller on paper and in electronic form. Storage of the paper form is stored in the file of the client or

employee, in printed form, in a closet at the company's office, which is in a physically enclosed place that is protected by a closed door.

Data stored in electronic form is stored by the data controller on a central computer located in the institution's offices, using hard drives and cloud services provided by a cloud service provider. With regard to the security of the cloud service, the data controller has performed the necessary compliance qualification audits of the provider's data security procedures.

- **Privacy incident, data protection supervision and remedies**

In Hungary, the Data Protection Supervisory Authority:

Hungarian National Authority for Data Protection and Freedom of Information

(hereinafter: NAIH, address: 1055 Budapest, Falk Miksa utca 9-11., e-mail address: ugyfelszolgalat@naih.hu

The subject may submit a complaint to the NAIH if he / she considers that the personal data management does not comply with legal obligations.

A judicial review may be initiated against NAIH's decision.

A privacy incident is a breach of data security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to the managed personal data. The data controller shall ensure the data security of the degree of risk associated with the data handling. In a case of a privacy incident,, no later than within 72 hours of the date of the incident, the data controller or it's representative shall notify the supervisory authority and inform the data subjects affected as well. The data controller shall promptly take the necessary security measures as soon as it becomes aware of the privacy incident to terminate the breach of the data protection and to restore the security of the managed data and restore the affected data to a state before the incident, or at least to the most intact state as possible. The subject will be notified of the measures taken and their results.

- **The name and contact information of the data controller**

Name: Hetedhét Ország Alapítvány (Mr. Peter Jones Foundation director)

Seat: 1124 Budapest, Fodor utca 36.

Contact information: info@happykids.hu