# THE HUGO SOFT „LIMITED LIABILITY COMPANY" PRIVACY POLICY

November 2, 2023.

**TABLE OF CONTENTS**

## I. Introduction, purpose and scope of the Code

### Introduction

Name of data controller organisation: Hugo Soft Kft.
Seat: 6000 Kecskemét, Úrihegy u. 44.
Company registration number: 03-09-137749
Tax number: 32380772-2-03
Availability: info@pinky-stories.org
Name and contact details of the authorized representative: Ugocsai Kristóf

The Data Controller sets out in this privacy policy ("Policy") how it collects, uses, stores, discloses or transfers personal data of its customers and partners. The Controller declares that this Policy complies in full with all applicable data protection rules and policies.

This Policy applies to all processing carried out by the Data Controller.

The Data Controller is entitled to unilaterally amend the Policy and any annexes thereto at any time and will inform its partners of such changes on its website.

In the event of any questions regarding the processing of any data by the Data Controller, the Data Controller will provide information to the requester at any of the contact details indicated, within the limits of the law.

The Policy and its annexes shall enter into force on 2 November 2023 and shall remain applicable until changed by the Data Controller.

This Privacy Policy will be reviewed and maintained in the light of changes in legislation, but at least annually.

### Purpose and scope of the Rules

*The purpose of* this Privacy Policy *is to* set out the internal rules of the Data Controller setting out its data protection and data management policy in compliance with the data protection and data management provisions set out in "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Regulation (EC) No 95/46/EC (General Data Protection Regulation)" . By enforcing these provisions, the Data Controller shall ensure, in all its activities and services, that the data subjects' right to the protection of their personal data is respected when processing or handling their personal data.

By adopting this Policy, the Data Controller declares its compliance with the principles for the processing of personal data set out in Article 5 of REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (hereinafter "the Regulation").

This Policy also aims to comply with the Hungarian data protection legislation, in the framework of which this Policy aims to comply with the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: Info Act). In drafting the Policy and its annexes, the Data Controller has taken into account all applicable legal provisions, compliance with which is relevant for data protection rules.

*The personal scope of* this Policy extends to the Data Controller and the natural persons in relation to whom the data processing activities of the Data Controller are carried out. The processing activities

set out in this Policy are directed at the personal data of natural persons. This Policy does not cover processing that relates to legal persons or, in particular, to undertakings that are incorporated as legal persons, including the name and form of the legal person and the contact details of the legal person. A legal person is an association, a partnership, a cooperative, an association and a foundation.

These Rules shall *apply* from the date of their entry into force until any further provision or until the date of their withdrawal.

## II. Definitions

**"personal data" and "data subject" means** any information ("personal data") relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
**'processing'** means any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
**"restriction of processing"** means the marking of stored personal data for the purpose of restricting their future processing;
**"profiling"** means any form of automated processing of personal data whereby personal data are used to evaluate or predict certain personal aspects relating to a natural person, in particular to analyze or predict characteristics associated with the work performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements of that natural person;
**"pseudonymisation"** means the processing of personal data in such a way that it is no longer possible to identify the natural person to whom the personal data relate without further information, provided that such further information is kept separately and technical and organizational measures are taken to ensure that no association with identified or identifiable natural persons is possible;
**"filing system"** means a set of personal data, structured in any way, whether centralized, decentralized or structured according to functional or geographical criteria, which is accessible on the basis of specified criteria;
**'controller'** means a natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of the processing are determined by Union or Member State law, the controller or specific criteria for the designation of the controller may also be determined by Union or Member State law;
**"data processor" means a** natural or legal person, public authority, agency or any other body which processes personal data on behalf of and for the account of the controller (on the controller's instructions and in accordance with the provisions of a contract with the controller);
**"recipient"** means a natural or legal person, public authority, agency or any other body to whom or with which personal data are disclosed, whether or not a third party. Public authorities which may have access to personal data in the context of an individual investigation in accordance with Union or Member State law are not recipients; the processing of those data by those public authorities must comply with the applicable data protection rules in accordance with the purposes of the processing;
**"third party"** means a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor or the persons who, under the direct authority of the controller or processor, are authorized to process personal data;
**"the data subject's consent"** means a freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject signifies, by a statement or by an act expressing his or her unambiguous consent, that he or she signifies his or her agreement to the processing of personal data concerning him or her;

**"data breach"** means a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
**"genetic data"** means any personal data relating to the inherited or acquired genetic characteristics of a natural person which contains specific information about the physiology or state of health of that person and which results primarily from the analysis of a biological sample taken from that natural person;
**'biometric data'** means any personal data relating to the physical, physiological or behavioral characteristics of a natural person obtained by means of specific technical procedures which allow or confirm the unique identification of a natural person, such as facial image or dactyloscopic data;
**"health data"** means personal data relating to the physical or mental health of a natural person, including data relating to the provision of health services to a natural person which contains information about the health of the natural person;
**"enterprise"** means any natural or legal person carrying on an economic activity, regardless of its legal form, including partnerships or associations carrying on a regular economic activity.

## III. Principles

*This section sets out the principles that the Data Controller will follow throughout the duration of its processing and in all its activities. The Principles are the rules and benchmarks that govern and define the processing as a whole.*

1. Personal data may only be processed for specified purposes and on a legal basis, for the exercise of a right or the performance of an obligation.
2. At all stages of processing, the purpose of the processing must be fulfilled and the collection and processing of data must be fair and lawful. Only personal data which is necessary for the purpose of the processing and is adequate for the purpose shall be processed.
3. Personal data may only be processed to the extent and for the duration necessary for the purpose.
4. The Data Controller records that the personal data it processes are stored at Hamburg, Germany Zone Name: eu-central-1-ham-1a Parent Region: Europe (Frankfurt) in the form of electronic files, in compliance with the legal requirements on data security. This provision applies to all processing and data processing activities carried out by the Controller.
The Data Controller shall process the data lawfully and fairly and in a transparent manner for the data subject (lawfulness, fairness and transparency).
The Data Controller shall collect personal data only for specified, explicit and legitimate purposes and shall not process them in a way incompatible with those purposes (purpose limitation), and shall not carry out any processing activity on the data after the purpose of the processing has been fulfilled.
7. The Data Controller shall carry out processing that is adequate, relevant and limited to what is necessary for the purpose(s) for which it is intended (data economy). Accordingly, the Data Controller shall not collect or store more data than is strictly necessary for the purpose of the processing.
8. The Data Controller's data management is accurate and up-to-date. The Data Controller shall take all reasonable steps to ensure that personal data inaccurate for the purposes of the processing are erased or rectified without undue delay (accuracy).
9. The Controller shall store personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, subject to the storage obligations laid down in the applicable legislation (limited storage).
10. The Data Controller shall ensure adequate security of personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage to personal data (integrity and confidentiality), by implementing appropriate technical or organizational measures.
11. The Data Controller is responsible for compliance with the principles detailed above and for demonstrating such compliance (accountability). Accordingly, the Data Controller shall ensure the ongoing implementation of these internal rules, the continuous review of its data management and, where necessary, the amendment and supplementation of data management procedures. The

Controller shall, where necessary, prepare documentation to demonstrate compliance with legal obligations.

## IV. Legal basis for processing

This section describes briefly and to the point when the Data Controller's (and any business's) processing may be lawful. In order to establish the lawfulness of processing, one or more legal grounds, i.e. an event/legal provision/circumstance/authorisation which renders the processing lawful by operation of law, are necessary. These legal grounds are briefly described below.

*1. Consent of the data subject*

- The lawfulness of the processing of personal data must be based on the consent of the data subject or on some other legitimate basis established by law.
- In the case of processing based on the data subject's consent, the data subject may give his or her consent to the processing of his or her personal data in the following form:
    a) in writing, in the form of a declaration of consent to personal data processing,
    (b) by electronic means, by any explicit conduct on the Controller's website, by ticking a box, or by making technical settings when using information society services, or by any other statement or action which, in the relevant context, unambiguously indicates the data subject's consent to the intended processing of his or her personal data.
- Silence, ticking a box or inaction does not constitute consent.
- Consent covers all processing activities carried out for the same purpose or purposes.
- Where the processing is intended for more than one purpose, consent must be given explicitly for all the purposes for which the processing is intended.
- Where the data subject gives his or her consent following an electronic request, the request must be clear and concise and must not unnecessarily impede the use of the service for which consent is sought.
- The data subject has the right to withdraw his or her consent at any time. Withdrawal of consent shall not affect the lawfulness of processing based on consent prior to its withdrawal. The data subject shall be informed before consent is given. The withdrawal of consent shall be made possible in the same simple manner as the giving of consent.

*2. Performance of the contract*

- Processing is lawful where it is necessary for the performance of a contract to which the data subject is a party or for the purposes of taking steps at the request of the data subject prior to entering into the contract.
- The consent of the data subject to the processing of personal data not necessary for the performance of the contract shall not be a condition for the conclusion of the contract.

*3. To comply with a legal obligation to which the controller is subject or to protect the vital interests of the data subject or of another natural person*

- The legal basis for processing is determined by law in the case of the performance of a legal obligation, so the data subject's consent is not required for the processing of his or her personal data.
- The Data Controller shall inform the data subject of the purposes, legal basis, duration and identity of the data controller, as well as of the data subject's rights and remedies.
- The Data Controller is entitled to process the data set which is strictly necessary for the fulfillment of a legal obligation to which the data subject is subject, following the withdrawal of the data subject's consent.

*4. the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or the legitimate interests of the controller or a third party.*

- The legitimate interests of the Controller, including the controller with whom the personal data may be shared, or of a third party may constitute a legal ground for processing, provided that the interests,

fundamental rights and freedoms of the data subject do not override the legitimate interests of the data subject, taking into account the reasonable expectations of the data subject in his or her relationship with the Controller. Such legitimate interest may, for example, be the case where there is a relevant and appropriate relationship between the data subject and the controller, such as where the data subject is a client of the controller or is employed by the controller.
- In order to establish the existence of a legitimate interest, it is necessary to carefully assess, inter alia, whether the data subject could reasonably expect, at the time and in the context of the collection of personal data, that processing for the purposes in question would take place.
- The interests and fundamental rights of the data subject may override the interests of the Controller if the personal data are processed in circumstances in which the data subjects do not expect further processing.

## V. General information on data management

As a basic principle, the Data Controller processes and uses the personal data of the natural person concerned in order to provide the services used by the data subject, to provide the services to an adequate standard and to improve the experience of the data subject.

In particular, the Data Controller processes data in connection with the activities (groups of activities) and cases listed below:
- the processing of data (visitor-related processing, registration, newsletter, order/purchase) carried out by the Data Controller in the course of the activities and services provided in connection with the operation of the website https://pinky-stories.org/
- processing of data in the course of the economic activities of the Data Controller (processing based on legal obligations, contact management, performance of contracts)
- data processing in the context of employment law and employment relationships.

The Data Controller does not employ a Data Protection Officer. If any data subject has any questions regarding data processing, he or she may contact the Data Controller using one of the contact details indicated in Section I of this Policy. In the event of a request, the Controller shall act in accordance with the procedure indicated in these Rules (see "Procedure to be followed in the event of a request by the data subject").

The detailed rules for the processing of data in connection with the activities referred to in this point (in particular: scope of data processed, purpose and legal basis of processing, duration of processing) are set out in the general provisions set out in the points set out below in these Rules and in the information documents annexed to these Rules, which contain detailed rules for the processing of data in the course of each activity. In the event of rules not specifically laid down in the information documents containing the detailed rules, the general provisions of these Rules shall prevail. These Rules and the individual information notices shall in all cases be interpreted and applied together, in a consistent and complementary manner. Each shall be indivisible from the other.

## VI. Processing of data relating to websites operated by the Data Controller

As stated in the previous section V, the Data Controller operates the following websites:
- the https://pinky-stories.org website;

The scope of data processing carried out by the Data Controller in the operation of the website can be defined as follows:
- processing of data relating to visitors to the Sites ("cookie"/customer data processing)
- registration
- newsletter service
- publication of advertisements

- order / website purchase
-messaging system
- marketing

We inform the data subjects that the specific and detailed rules for each processing operation (the so-called processing circles) in the course of the processing referred to in this point VI are set out in the *Information Notice* ("Information Notice on the processing of personal data on the websites operated by the Controller"), which *is Annex 1 to* these Rules. The said Notice describes in detail the processing of data under this point. The Prospectus shall be read in conjunction with and in accordance with this Policy at all times. The general provisions of this Policy shall prevail in respect of any matter not covered by the Policy and not specifically set out in the Policy.

**VII. Processing of data in the course of the economic activities of the Data Controller**

In the course of its economic activity, the Data Controller also carries out processing in addition to the previous point. These are data processing activities that generally occur in most companies. However, their general occurrence does not mean that you should not be informed of them. It is true that, also in relation to the processing referred to in this point, the Data Controller will make every effort to ensure that the personal data of all data subjects are kept secure and that the processing of such data also complies in all respects with the applicable data protection rules and policies.

The specific categories of processing under this point which are/may be separately identified:
- processing based on a legal obligation
- contacting
- performance of contracts

We inform the data subjects that the specific and detailed rules of the individual processing operations (the so-called processing circles) carried out in the course of the processing referred to in this point VII are set out in the *Information Notice* ("Information Notice on the Processing of Data in Connection with the Controller's Business Activities"), which *is Annex 2 to* these Rules. The said Notice describes in detail the processing under this point. The Prospectus shall at all times be read in conjunction with and in accordance with these Rules. The general provisions of this Policy shall prevail in relation to any matter not covered by the Prospectus.

**VIII. Data processing in connection with employment law and employment relationships**

The Data Controller wishes to inform the data subjects that, as a general rule, it only publishes job advertisements together with their identity.

The Data Controller informs the data subjects that their application materials (CV, cover letter, any attachments and other documents) will be stored and kept for a maximum of 12 months from the date of receipt. The storage is done in order to use the data subjects' application materials to meet the recruitment needs of the Data Controller. Accordingly, the Data Controller may contact the person concerned, i.e. the candidate who has applied for the vacancy, with further job offers for which the candidate is suitable for the position for a maximum period of 12 months after the submission of the application.

If a data subject does not submit his/her application to the Data Controller within the framework of an application for a specific advertised position, the Data Controller shall request written confirmation and consent from the data subject within a reasonable period of time, but not more than 5 working days, that the Data Controller may store and use the application and the personal data of the data subject in accordance with this clause. If no consent is received from the candidate within the time limit, the Data

Controller shall delete the application and all personal data of the data subject from its system without any further action.

The Data Controller, as (prospective) employer, will inform the data subjects about the provisions of this point separately in the context of each job advertisement.

It can therefore be stated that the purpose of the data processing recorded so far in this section is the recruitment of the data subjects as applicants/prospective employees and the conclusion of the employment contract with them. The legal basis for the processing is the consent of the data subject. The scope of the data processed is the necessary data indicated in each job advertisement which are relevant for the assessment of the application (in particular, but not exclusively: CV data, data of documents proving qualifications, contact details, etc.). The recipients of the personal data are the employer, the employee(s) of the Data Controller performing the human resources function and, where applicable, the data processor(s) entrusted with the performance of the HR tasks and acting on the instructions of the Data Controller.

The specific and detailed rules on further data processing (data processing categories) relating to employees are set out in the *Information Notice* ("Information on data processing in the context of employment law and employment relationships"), which *is Annex 3 to* these Rules. The said Notice describes in detail the processing of data under this point. The Prospectus shall be read in conjunction with and in accordance with these Rules at all times. The general provisions of this Policy shall prevail in relation to any matter not covered by the Prospectus. Please note that the information referred to in this point is not public and will be communicated by the Data Controller only to the persons concerned.

## IX. Rights of the data subject

*1. (Prior) Right to information*
(1) The data subject shall have the right to be informed of the essential information relating to the processing of his or her data before the processing of the data is started.

(2) Information to be provided where personal data are collected from the data subject:

a. the identity and contact details of the controller and, where applicable, the controller's representative;
b. the contact details of the Data Protection Officer, if any;
c. the purposes for which the personal data are intended to be processed and the legal basis for the processing;
d. in the case of processing based on Article 6(1)(f) of the Regulation, the legitimate interests of the controller or a third party;
e. where applicable, the recipients of the personal data and the categories of recipients, if any;
f. where applicable, the fact that the controller intends to transfer the personal data to a third country or an international organization and the existence or absence of an adequacy decision by the Commission or, in the case of a transfer referred to in Article 46, Article 47 or the second subparagraph of Article 49(1) of the Regulation, an indication of the appropriate and adequate safeguards and a reference to the means of obtaining a copy or the availability of a copy.

(3) In addition to the information referred to in paragraph 1, the controller shall, at the time of obtaining the personal data, in order to ensure fair and transparent processing, provide the data subject with the following additional information:

a. the duration of the storage of personal data or, where this is not possible, the criteria for determining that duration;

b. the right of the data subject to request the controller to access, rectify, erase or restrict the processing of personal data concerning him or her and to object to the processing of such personal data, and the right to data portability;
c. in the case of processing based on Article 6(1)(a) or Article 9(2)(a) of the Regulation, the right to withdraw consent at any time, without prejudice to the lawfulness of the processing carried out on the basis of consent prior to its withdrawal;
d. the right to lodge a complaint with a supervisory authority;
e. whether the provision of the personal data is based on a legal or contractual obligation or is a precondition for the conclusion of a contract, whether the data subject is under an obligation to provide the personal data and the possible consequences of not providing the data;
f. the fact of automated decision-making, including profiling, as referred to in Article 22(1) and (4) of the Regulation, and, at least in those cases, clear information on the logic used and the significance of such processing and its likely consequences for the data subject.

(4) Where the personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

a. the identity and contact details of the controller and, where applicable, the controller's representative;
b. the contact details of the Data Protection Officer, if any;
c. the purposes for which the personal data are intended to be processed and the legal basis for the processing;
d. the categories of personal data concerned;
e. the recipients of the personal data and the categories of recipients, if any;
f. where applicable, the fact that the controller intends to transfer the personal data to a recipient in a third country or to an international organization and the existence or absence of an adequacy decision by the Commission or, in the case of a transfer referred to in Article 46, Article 47 or the second subparagraph of Article 49(1) of the Regulation, an indication of the appropriate and suitable safeguards and a reference to the means of obtaining a copy or their availability.

(5) In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following additional information necessary to ensure fair and transparent processing for the data subject:

a. the duration of the storage of personal data or, where this is not possible, the criteria for determining that duration;
b. where the processing is based on Article 6(1)(f) of the Regulation, the legitimate interests of the controller or a third party;
c. the right of the data subject to request the controller to access, rectify, erase or restrict the processing of personal data concerning him or her and to object to the processing of personal data, and the right to data portability;
d. in the case of processing based on Article 6(1)(a) or Article 9(2)(a) of the Regulation, the right to withdraw consent at any time, without prejudice to the lawfulness of the processing carried out on the basis of consent prior to its withdrawal;
e. the right to lodge a complaint with a supervisory authority;
f. the source of the personal data and, where applicable, whether the data originate from publicly available sources; and
g. the fact of automated decision-making, including profiling, as referred to in Article 22(1) and (4) of the Regulation and, at least in those cases, the logic used and clear information on the significance of such processing and its likely consequences for the data subject.

(6) If the controller intends to further process personal data for a purpose other than that for which they were obtained, the controller shall inform the data subject of that other purpose and of any relevant additional information referred to above before further processing.
(7) Paragraphs (1) to (6) do not apply if and to the extent that:

a. the data subject already has the information;
b. the provision of the information in question proves impossible or would involve a disproportionate effort, in particular in the case of processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, taking into account the conditions and guarantees referred to in Article 89(1), or where the obligation referred to in paragraph 1 of this Article would be likely to render impossible or seriously impair the achievement of the purposes of such processing. In such cases, the controller shall take appropriate measures, including making the information publicly available, to protect the rights, freedoms and legitimate interests of the data subject;
c. the acquisition or disclosure of the data is expressly required by Union or Member State law applicable to the controller, which provides for appropriate measures to protect the data subject's legitimate interests; or
d. the personal data must remain confidential under an obligation of professional secrecy imposed by EU or Member State law, including a legal obligation of secrecy.

*2. Right of access of the data subject*
(1) The data subject shall have the right to obtain from the controller feedback as to whether or not his or her personal data are being processed and, if such processing is taking place, the right to access the personal data and the following information:

a. the purposes of the processing;
b. the categories of personal data concerned;
c. the recipients or categories of recipients to whom or with whom the personal data have been or will be disclosed, including in particular recipients in third countries or international organizations;
d. where applicable, the envisaged period of storage of the personal data or, if this is not possible, the criteria for determining that period;
e. the right of the data subject to obtain from the controller the rectification, erasure or restriction of the processing of personal data concerning him or her and to object to the processing of such personal data;
f. the right to lodge a complaint with a supervisory authority;
g. if the data were not collected from the data subject, any available information on their source;
h. the fact of automated decision-making, including profiling, as referred to in Article 22(1) and (4) of the Regulation and, at least in those cases, the logic used and clear information on the significance of such processing and its likely consequences for the data subject.

(2) Where personal data are transferred to a third country or an international organization, the data subject shall have the right to be informed of the appropriate safeguards for the transfer in accordance with Article 46.
(3) The data controller shall provide the data subject with a copy of the personal data processed upon request/request. For additional copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject has made the request by electronic means, the information shall be provided in a commonly used electronic format, unless the data subject requests otherwise.

*3. The data subject's right to rectification and erasure*

3.1. Right to rectification

(1) The data subject shall have the right to obtain, upon his or her request and without undue delay, the rectification of inaccurate personal data relating to him or her. Having regard to the purposes of the processing, the data subject shall have the right to obtain the rectification of incomplete personal data, including by means of a supplementary declaration.

3.2 Right to erasure ("right to be forgotten")

(1) The data subject shall have the right to obtain from the controller the erasure of personal data relating to him or her without undue delay at his or her request and the controller shall be obliged to erase personal data relating to him or her without undue delay where one of the following grounds applies:

a. the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
b. the data subject withdraws his or her consent pursuant to Article 6(1)(a) of the Regulation (consent to the processing of personal data) or Article 9(2)(a) of the Regulation (explicit consent), and there is no other valid legal basis for the processing;
c. the data subject objects to the processing on the basis of Article 21(1) of the Regulation (right to object) and there is no overriding legitimate ground for the processing, or the data subject objects to the processing on the basis of Article 21(2) of the Regulation (objection to processing for commercial purposes);
d. the personal data have been unlawfully processed;
e. the personal data must be erased in order to comply with a legal obligation under Union or Member State law to which the controller is subject;
f. personal data have been collected in connection with the provision of information society services referred to in Article 8(1).

(2) Where a controller has disclosed personal data and is required to erase it at the request of the data subject, it shall take reasonable steps, including technical measures, taking into account the available technology and the cost of implementation, to inform the controllers that process the data that the data subject has requested the deletion of the links to or copies or replicas of the personal data in question.

(3) Paragraphs (1) and (2) shall not apply where the processing is necessary:

a. to exercise the right to freedom of expression and information;
b. for the purposes of complying with an obligation under Union or Member State law to which the controller is subject to which the processing of personal data is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c. on grounds of public interest in the field of public health pursuant to Article 9(2)(h) and (i) of the Regulation and Article 9(3) of the Regulation;
d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the Regulation, where the right referred to in paragraph 1 would be likely to render such processing impossible or seriously impair it; or
e. to bring, enforce or defend legal claims.

*4. Right to restriction of processing*

(1) The data subject shall have the right to obtain, at his or her request, restriction of processing by the controller if one of the following conditions is met:

a. the data subject contests the accuracy of the personal data, in which case the restriction applies for the period of time necessary to allow the controller to verify the accuracy of the personal data;
b. the data processing is unlawful and the data subject opposes the erasure of the data and requests instead the restriction of their use;
c. the controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defense of legal claims; or

d. the data subject has objected to the processing pursuant to Article 21(1) of the Regulation; in this case, the restriction shall apply for the period until it is established whether the legitimate grounds of the controller override those of the data subject.

(2) Where processing is restricted pursuant to paragraph 1, such personal data may be processed, except for storage, only with the consent of the data subject or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or of an important public interest of the Union or of a Member State.

(3) The controller shall inform the data subject at whose request the processing has been restricted pursuant to paragraph (1) in advance of the lifting of the restriction.

*5. Obligation to notify the rectification or erasure of personal data or the restriction of processing*

(1) The controller shall inform all recipients to whom or with whom the personal data have been disclosed of the rectification, erasure or restriction of processing, unless this proves impossible or involves a disproportionate effort.

(2) At the request of the data subject, the controller shall inform him or her of the recipients.

*6. The right to data portability*

(1) The data subject shall have the right to receive personal data relating to him or her which he or she has provided to a controller in a structured, commonly used, machine-readable format and the right to transmit those data to another controller without hindrance from the controller to whom the personal data have been provided, if:

a. the processing is based on consent pursuant to Article 6(1)(a) of the Regulation (consent to the processing of personal data) or Article 9(2)(a) of the Regulation (explicit consent to processing) or on a contract pursuant to Article 6(1)(b); and
b. the processing is carried out by automated means.

(2) In exercising the right to data portability under paragraph (1), the data subject shall have the right to request, where technically feasible, the direct transfer of personal data between controllers.

(3) The exercise of the right referred to in paragraph (1) of this Article shall be without prejudice to Article 17 of the Regulation. That right shall not apply where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

(4) The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

*7. The right to object*

(1) The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to processing of his or her personal data carried out in the exercise of his or her official authority or in the public interest or to processing necessary for the purposes of the legitimate interests pursued by the controller or by a third party (processing based on Article 6(1)(e) or (f) of the Regulation), including profiling based on those provisions. In such a case, the controller may no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

(2) Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such purposes, including profiling, where it is related to direct marketing.

(3) If the data subject objects to the processing of personal data for direct marketing purposes, the personal data shall no longer be processed for those purposes.

(4) The right referred to in paragraphs (1) and (2) shall be explicitly brought to the attention of the data subject at the latest at the time of the first contact with the data subject and the information shall be clearly displayed separately from any other information.

(5) In the context of the use of information society services and by way of derogation from Directive 2002/58/EC, the data subject may exercise the right to object by automated means based on technical specifications.

(6) Where personal data are processed for scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the Regulation, the data subject shall have the right to object, on grounds relating to his or her particular situation, to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

*8. Right to exemption from automated decision-making*

(1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

(2) Paragraph (1) shall not apply where the decision:

a. necessary for the conclusion or performance of a contract between the data subject and the controller;
b. is permitted by Union or Member State law applicable to the controller which also lays down appropriate measures to protect the rights and freedoms and legitimate interests of the data subject; or
c. is based on the explicit consent of the data subject.

(3) In the cases referred to in points (a) and (c) of paragraph 2, the controller shall take appropriate measures to safeguard the rights, freedoms and legitimate interests of the data subject, including at least the right to obtain human intervention by the controller, to express his or her point of view and to object to the decision.

(4) The decisions referred to in paragraph (2) shall not be based on the special categories of personal data referred to in Article 9(1) of the Regulation, unless Article 9(2)(a) or (g) applies and appropriate measures have been taken to safeguard the rights, freedoms and legitimate interests of the data subject.

*9. Right of the data subject to lodge a complaint and seek redress*

9.1 Right to lodge a complaint with a supervisory authority.

(1) The data subject shall have the right to lodge a complaint with the supervisory authority pursuant to Article 77 of the Regulation if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

(2) The data subject may exercise his or her right to lodge a complaint by contacting:

- Hungarian National Authority for Data Protection and Freedom of Information - address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.; telephone: +36 (1) 391-1400; fax: +36 (1) 391-1410; website: http://www.naih.hu; e-mail: ugyfelszolgalat@naih.hu.

(3) The supervisory authority with which the complaint has been lodged shall inform the client of the procedural developments concerning the complaint and of the outcome thereof, including the right of the client to seek judicial remedy pursuant to Article 78 of the Regulation.

9.2 Right to an effective judicial remedy against the supervisory authority

(1) Without prejudice to any other administrative or non-judicial remedy, any natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of the supervisory authority concerning him.

(2) Without prejudice to other administrative or non-judicial remedies, any person concerned shall have the right to an effective judicial remedy if the competent supervisory authority does not deal with the complaint or does not inform the person concerned within three months of the procedural developments concerning the complaint lodged pursuant to Article 77 of the Regulation or of the outcome of the complaint.

(3) Proceedings against a supervisory authority shall be brought before the courts of the Member State in which the supervisory authority is established.

(4) If proceedings are brought against a decision of a supervisory authority on which the Board has previously issued an opinion or taken a decision under the consistency mechanism, the supervisory authority shall send that opinion or decision to the court.

9.3 Right to an effective judicial remedy against the controller or processor

(1) Without prejudice to the administrative or non-judicial remedies available, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, any data subject shall have an effective judicial remedy if he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data not in accordance with this Regulation.

(2) Proceedings against a controller or processor shall be brought before the courts of the Member State in which the controller or processor is established. Such proceedings may also be brought in the courts of the Member State in which the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in its exercise of official authority.

*10. Restrictions*

(1) Union or Member State law applicable to a controller or processor may, by legislative measures, limit the scope of the rights and obligations set out in Article 5 in respect of its provisions in Articles 12 to 22 and Article 34 and in accordance with the rights and obligations set out in Articles 12 to 22, if the limitation respects the essential content of fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to protect them:

a. national security;
b. defence;
c. public safety;
d. the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the protection against and prevention of threats to public security;
e. other important objectives of general interest of the Union or of a Member State, in particular important economic or financial interests of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
f. the independence of the judiciary and the protection of judicial procedures;
g. prevent, investigate, detect and prosecute ethical violations in regulated professions;
h. in the cases referred to in points (a) to (e) and (g), even occasionally, control, inspection or regulatory activities connected with the exercise of official authority;
i. to protect the data subject or to protect the rights and freedoms of others;
j. enforce civil claims.

(2) The legislative measures referred to in paragraph 1 shall contain, where appropriate, at least detailed provisions:

a. the purposes or categories of processing,
b. categories of personal data,
c. the scope of the restrictions imposed,
d. safeguards to prevent misuse or unauthorized access or disclosure,
e. to define the controller or to define categories of controllers,
f. the duration of storage and the applicable safeguards, taking into account the nature, scope and purposes of the processing or categories of processing,
g. the risks to the rights and freedoms of data subjects, and
h. the right of data subjects to be informed of the restriction, unless this might undermine the purpose of the restriction.

*11. Information about the data breach*

(1) Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall inform the data subject of the personal data breach without undue delay.

(2) The information referred to in paragraph 1 provided to the data subject shall clearly and prominently describe the nature of the personal data breach and shall include at least the name and contact details of the data protection officer or other contact person who will provide further information, the consequences of the personal data breach and the likely consequences, the

measures taken or envisaged by the controller to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the personal data breach.
(3) The data subject need not be informed as referred to in paragraphs (1) to (2) if any of the following conditions are met:

a. the data controller has implemented appropriate technical and organizational protection measures and these measures have been applied to the data affected by the personal data breach, in particular measures, such as the use of encryption, which render the data unintelligible to persons not authorized to access the personal data;
b. the controller has taken additional measures following the personal data breach to ensure that the high risk to the rights and freedoms of the data subject referred to in paragraph 1 is no longer likely to materialize;
c. information would require a disproportionate effort. In such cases, the data subjects should be informed by means of publicly disclosed information or by a similar measure which ensures that the data subjects are informed in an equally effective manner.

(4) Where the controller has not yet notified the data subject of the personal data breach, the supervisory authority may, after having considered whether the personal data breach is likely to present a high risk, order the data subject to be informed or determine that one of the conditions referred to in paragraph 3 is met.

## X. Procedure to be followed in the event of a request by the data subject

- The Data Controller is committed to protecting the rights of data subjects. To this end, it will do its utmost to ensure that the rights of data subjects are exercised to the fullest extent possible and that they are not adversely affected.
- The Data Controller shall facilitate the exercise without difficulty by any data subject of his or her rights under the law and the directives that are intended to ensure the protection of his or her personal data.
- The Data Controller may not refuse to comply with a request to exercise the rights of the data subject as set out in this Policy, unless the Data Controller proves that it is not possible to identify the data subject.
- The Data Controller shall inform the data subject of the action taken on the request without undue delay, but in any event within 15 (fifteen) working days of receipt of the request. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further (maximum) month. The Data Controller shall inform the data subject of the extension of the time limit within 15 (fifteen) working days of receipt of the request, stating the reasons for the delay.
- If the data subject has made the request by electronic means, the information shall be provided by electronic means where possible, unless the data subject requests otherwise.
- If the controller does not act on the data subject's request, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for the failure to act and of the right to lodge a complaint with the supervisory authority and to seek judicial remedy.
- The Data Controller shall provide the information and information requested free of charge to the data subject. However, where the data subject's request is manifestly unfounded or excessive, in particular because of its repetitive nature, the Controller may, taking into account the administrative costs of providing the information or information requested or of taking the action requested, charge a reasonable fee or refuse to act on the requestThe burden of proving that the request is manifestly unfounded or excessive lies with the Data Controller.)

## XI. Who has access to the data and the general rules on data processing

- The personal data of the data subjects may be accessed by the employees of the Data Controller with access rights related to the relevant processing purpose (and allocated by the employer), and by

persons and organizations performing data processing activities for the Data Controller on the basis of service contracts, to the extent and to the extent necessary for the performance of their activities, as determined by the Data Controller.
- Processors shall in all cases perform processing activities on behalf of and under the instructions of the Controller. Processors, unlike the Data Controller, are therefore not free to make their own decisions regarding the processing. Processors may not use personal data received from the Controller for their own purposes.
- The Data Controller shall monitor the work of the processors.
- Any data processor is entitled to use an additional data processor only if the Data Controller has given its prior written consent.
- The Data Controller records that it uses an external data processor, in particular in the cases listed below, in order to achieve the purposes listed below:

(i) operation, maintenance and hosting of Internet websites
(ii) tax and accounting obligations, invoicing software services, bookkeeping and payroll;
(iii) performance of contracts, delivery and transport;
(iiii) the use of IT and business management system services.

- A list of the data processors used by the Data Controller for any of its activities is set out in a separate document, *Annex 4 to* these Rules ("Register of Data Processors").

## XII Provisions on data security

*1. Principles for implementing data security*
- The Data Controller may process personal data only in accordance with the activities set out in this Policy and the Annexes and for the purposes for which they are processed.
- The Data Controller shall ensure the security of the data, and in this context undertakes to take all technical and organizational measures that are indispensable to enforce the laws on data security, data protection and confidentiality rules, and to establish the procedural rules necessary to enforce the above-mentioned laws.
- The technical and organizational measures to be implemented by the Data Controller shall be aimed in particular at:

a. pseudonymisation and encryption of personal data;
b. ensuring the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data;
c. in the event of a physical or technical incident, the ability to restore access to and availability of personal data in a timely manner;
d. the use of a procedure to regularly test, assess and evaluate the effectiveness of the technical and organizational measures taken to ensure the security of processing,

- In determining the appropriate level of security, explicit account should be taken of the risks arising from the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.
- The Data Controller shall take appropriate measures to protect the data against unauthorized access, alteration, disclosure, disclosure, erasure or destruction, accidental destruction or damage and inaccessibility resulting from changes in the technology used.
- The Data Controller shall keep records of the data processed by it in accordance with the applicable legislation, ensuring that the data may only be accessed by employees, other persons acting in the interests of the Data Controller and data processors who need to know the data in order to perform their job or task.
- The Data Controller shall store personal data provided in the course of each processing activity separately from other data, with the understanding that, in accordance with the above provisions, the separate data files may be accessed only by employees with appropriate access rights.
- The managers of the Data Controller, employees will not transmit personal data to third (unauthorized external) persons, and will take the necessary measures to prevent unauthorized access.

- The Data Controller shall allow access to personal data to those of its employees who have agreed to comply with the data security rules by signing a confidentiality statement in relation to the personal data processed.
- When determining and applying data security measures, the Data Controller shall take into account the state of the art and, where there are several possible processing solutions, shall choose the solution offering a higher level of protection of personal data, unless this would involve a disproportionate level of difficulty.

*2. Protection of the Company's IT records*
- The Data Controller shall take the following measures necessary to ensure the security of its IT records:
    a. Provide the data files it manages with permanent protection against computer viruses (using real-time virus protection software).
    b. Ensure the physical protection of the hardware assets of the IT system, including protection against elemental damage,
    c. Ensures that the IT system is protected against unauthorized access, both in terms of software and hardware,
    d. Take all measures necessary to restore data files, perform regular backups and ensure separate and secure management of backups.

*3. Protection of the Company's paper records*
- The Data Controller shall take the necessary measures to protect paper records, in particular with regard to physical security and fire protection.
- The Controller's managers, employees and other persons acting on behalf of the Controller shall keep secure and protect the data media containing personal data which they use or have in their possession, regardless of the means of recording the data, against unauthorized access, alteration, disclosure, disclosure, erasure or destruction and against accidental destruction or damage.

## XIII. Procedure in the event of a personal data breach

- A personal data breach is a breach of security within the meaning of the Regulation that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- A data breach is the loss or theft of a device (laptop, mobile phone) containing personal data, the loss or unavailability of a code to decrypt a file encrypted by the Data Controller, infection by ransomware (ransomware) that renders the data processed by the Data Controller inaccessible until the payment of a ransom, an attack on the IT system, the disclosure of an e-mail or address list containing personal data sent in error, etc.
- In case of detection of a data breach, the Data Controller's representative shall immediately conduct an investigation to identify the data breach and its possible consequences. The necessary measures shall be taken to remedy the damage.
- You must notify the data protection incident to the competent supervisory authority without undue delay and, if possible, no later than 72 hours after becoming aware of the data protection incident, unless the data protection incident is unlikely to pose a risk to the rights and freedoms of natural persons. If the notification is not made within 72 hours (although it is necessary), it must be accompanied by the reasons justifying the delay.
- If the data processor becomes aware of a data breach, it shall notify the Data Controller without undue delay after becoming aware of it.
- In the notification referred to in paragraph 4, at least:
    a. describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects and the categories and approximate number of data subjects affected by the breach;

b. the name and contact details of the Data Protection Officer or other contact person who can provide further information;
c. explain the likely consequences of the data breach;
d. describe the measures taken or envisaged by the Data Controller to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the personal data breach.

- If and to the extent that it is not possible to provide the information at the same time, it may be provided in instalments at a later date without further undue delay.
- The Data Controller shall keep a record of the data breaches, indicating the facts relating to the data breach, its effects and the measures taken to remedy it. This record shall enable the supervisory authority to verify compliance with the requirements of Article 33 of the Regulation.

## XIV. Other provisions

- The Data Controller's manager shall explain the provisions of this Policy to all employees of the Data Controller.
- The Controller's manager shall ensure that all employees of the Controller comply with the provisions of this Policy. For the purpose of implementing this obligation, the Controller's administrator shall require that the employment contracts of the Controller's employees be amended to include a declaration of the employee's commitment to comply with and enforce this Policy.
- The establishment and amendment of this Policy is the responsibility of the Data Controller's Chief Executive Officer.

## XV. Request, complaint, remedy

If any data subject has any questions or comments regarding the Data Controller's data management activities, he/she may submit his/her questions/requests/comments to the Data Controller at any of the contact details indicated in this Policy. Depending on the subject of the request, the Controller shall act in accordance with the provisions of these Rules.

*You can lodge a complaint or seek redress from the following bodies:*
National Authority for Data Protection and Freedom of Information Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
Website: http://www.naih.hu
E-mail: ugyfelszolgalat@naih.hu

In case of violation of the rights of minors in relation to offensive, hateful, exclusionary content, rectification, rights of a deceased person, defamation of reputation:
National Media and Infocommunications Authority 1015 Budapest, Ostrom u. 23-25.
Mailing address: 1525. Pf. 75
Tel: (06 1) 457 7100
Fax: (06 1) 356 5520
E-mail: info@nmhh.hu

The data subject may take legal action if his or her rights are infringed. The court will rule on the case out of turn. The Data Controller shall prove that the processing complies with the law. The competent court has jurisdiction to rule on the case. In addition to the general rule of jurisdiction, the place of residence or habitual residence of the data subject shall be a ground for the jurisdiction of the court.

In the event that the Data Controller infringes the personal rights of the data subject by unlawful processing of the data subject's data or by breaching the requirements of data security, the data subject may claim damages or compensation from the Data Controller.

**XVII Annexes**

*Annex 1:* "Information on data management on the websites operated by the Data Controller"

November 2, 2023

**Hugo Soft Kft.**

**INFORMATION ON DATA MANAGEMENT IN RELATION TO WEBSITES OPERATED BY THE CONTROLLER**

This Notice shall be deemed to be Annex 1 to the Controller's Policy ("General Data Protection Policy"). This Notice describes in detail the processing of data related to the activities of the Controller in relation to its websites. This Notice shall be read in conjunction with and in accordance with the relevant Policy and its Annexes. For matters not covered by this Policy, the general provisions of the Policy and the specific provisions of the additional annexes shall prevail.

1. Introduction

Name of the Data Controller Entities: Hugo Soft Korlátolt Felelősségű Társaság
Registered office.
Company registration number: 03-09-137749
Tax number: 32380772-2-03
Contact: info@pinky-stories.org
Name and contact details of the authorised representative: Ugocsai Kristóf, 6000 Kecskemét, Úrihegy u. 44.

Websites operated by the Data Controller:
- The website https://pinky-stories.org/;

- processing of data relating to visitors to the pages ("cookie"/south processing)
- registration
- newsletter service
- publication of advertisements
- placing an order / making a purchase on the website
- messaging system
- marketing

2. Processing of data relating to visitors to the site ("cookie"/customer data processing)

To provide you with a convenient browsing and shopping experience, we use cookies/cookies to provide content, to analyze our website and for possible advertising.

2.1 General information
- During the visits to the website of the Data Controller, one or more cookies are sent to the computer of the person visiting the website, through which his/her browser(s) will be identified, provided that the

person visiting the website has given his/her explicit (active) consent to this in advance, after having been clearly and unambiguously informed, by his/her behaviour for further browsing of the website.
- A "cookie", also known as a "cookie", is a small packet of information that is sent by the server to the browser and then returned by the browser to the server whenever a request is directed to the server.
- Cookies work solely to improve the user experience and automate the login process. The cookies used on the website do not store personally identifiable information.
- Cookies are short data files placed on the user's computer by the website visited. The purpose of the cookie is to make the particular infocommunication, internet service easier and more convenient. There are several types, but they generally fall into two broad categories. One is the temporary cookie, which is placed on the user's device by the website only during a particular session (e.g. during the security identification of an online banking transaction), and the other is the persistent cookie (e.g. a website's language setting), which remains on the computer until the user deletes it. According to the European Commission's guidelines, cookies [unless strictly necessary for the use of the service] can only be placed on the user's device with the user's permission.
- In the case of cookies that do not require the user's consent, information should be provided during the first visit to the website. It is not necessary for the full text of the cookie notice to appear on the website, but it is sufficient for website operators to provide a brief summary of the substance of the notice and a link to the full notice.
- In the case of cookies requiring consent, the information may also be linked to the first visit to the website, if the processing of data associated with the use of cookies starts as soon as the page is visited. Where the use of the cookie is linked to the use of a function explicitly requested by the user, the information may also be provided in relation to the use of that function. Even in this case, it is not necessary for the full text of the cookie notice to be displayed on the website, a brief summary of the substance of the notice and a link to the full notice.

2.2. Cookie settings
- As described above, cookies may be stored by our company as Data Controller on the data subject's (website visitor's) device if this is indispensable for the functioning of the website. In all other cases and for all other types of cookies, the prior explicit consent of the data subject is required for the use and storage of cookies.
- The Data Controller uses several types of cookies. Some of the cookies are placed on the data subject's device by the Data Controller, others are placed on the data subject's device by data processors or third party service providers.
- The data subject can review his or her current cookies in relation to the website currently visited by the Controller at any time via the relevant website under the "cookie policy" and change their settings. Data Subjects T are informed that when reviewing the cookies, they will be given the opportunity to obtain information on the exact name of the cookies used, the purpose of the cookie and the storage period of the cookie.
- In addition, browsers typically offer the possibility for the data subject to change their cookie settings. Changing cookie settings in the browser is usually done via the {menu} {preferences} {privacy and security} {cookies}.

2.3. Grouping of cookies used

2.3.1. Essential cookies

The website used by the data subject cannot function properly without essential cookies. Without these cookies, the data subject will not be able to use the website he or she visits.

2.3.2. Preferential, preference cookies

Preferential cookies allow us to remember information that changes the way the website behaves or looks (e.g. language preference, region preference, etc.)

2.3.3. Statistical cookies

Through the collection and reporting of data in an anonymous form, statistical cookies help the Data Controller to understand, analyze and make use of the way visitors (data subjects) interact with the website they visit.

2.3.4. Cookies for marketing purposes

We use personalized, marketing cookies to track visitors' website activity. The aim is to serve the most relevant ads to individual users, display content that is relevant to their preferences and encourage them to be active.

2.3.5. Unclassified cookies

Unclassified cookies are cookies that are still under classification with individual cookie providers.

2.4. Request for information
If any data subject has questions regarding the processing of cookies, he or she may request information via the contact details provided by the Data Controller.

3. Registration

(1) The legal basis for the processing is the voluntary consent of the data subject when registering, when registering on the Controller's website, the data subject obtains information on the processing of his/her data by clicking on the link embedded in the "Privacy Policy", while his/her explicit consent is given by ticking the box next to a.
(2) In the case of registration, the data subject is any natural person over the age of 18 who registers on the Controller's website and gives his or her consent to the processing of his or her personal data and declares that he or she is over the age of 18.
(3) The scope of the processed data in case of registration: username, e-mail address, password.
(4) The purpose of the processing in case of registration: contacting, preparing the conclusion of a contract, information on product listing, placing and receiving orders, providing the services available free of charge on the website to the data subject, access to the non-public content of the website, facilitating transactions between registered users.
(5) The recipients of the data (who may have access to the data) in the case of registration: the manager of the Controller, the staff of the Data Processor performing the tasks related to the operation of the website of the Controller, the staff of the Data Processor performing the tasks related to the operation of the website of the Controller.
(6) Duration of data processing in the case of registration: until consent is withdrawn or deleted at the request of the data subject.
(7) The data subject may request the deletion of his/her registration (personal data) at any time.

4. Newsletter service

(1) The legal basis for the processing is the voluntary consent of the data subject to subscribe to the newsletter, which the data subject gives by ticking the box(es) next to the text "subscribe to newsletter" on the Controller's website after being informed about the processing of his/her data.
(2) The data subject in the case of newsletter subscription: any natural person who subscribes to the newsletter of the Controller and gives his/her consent to the processing of his/her personal data.
(3) The scope of the processed data in case of newsletter subscription: name, e-mail address.

(4) Purpose of the processing in case of newsletter subscription: to inform the data subject about the services and products of the Data Controller, changes in them, news and events, sending commercial advertising, sending email messages/newsletters containing marketing enquiries.
(5) The recipients of the data (who may have access to the data) in the case of newsletter subscriptions: the Controller's manager, customer contact staff, staff performing the tasks related to the operation of the Controller's website and related tasks, staff of the data processor performing the tasks related to the operation of the Controller's website and related tasks.
(6) Duration of data processing in the case of newsletter subscriptions: until consent is withdrawn and until unsubscription.
(7) The data subject may unsubscribe from the newsletter at any time. The unsubscription to the newsletter is done by clicking on the unsubscribe link in the footer of the emails sent to the data subject, by post to the Data Controller's headquarters.

5. Publication of advertisements

(1) The Data Controller shall provide registered data subjects with a user account with the possibility to post advertisements related to product sales.
(2) The legal basis for the processing of data by the Data Controller in connection with the publication of advertisements is the conclusion of a contract to which the data subject is a party.
(3) The data subject is any natural person who is registered on the website and places an advertisement.
(5) The purposes of the processing: the management of the processing of data relating to the advertisements placed or the advertising started by the data subjects.
(6) Recipients of personal data: the Data Controller's manager, employees performing customer service and marketing tasks on the basis of their job function and data processors performing tasks in this context, employees of the data processor performing tasks related to the operation of the Data Controller's website and related tasks.
(7) The personal data processed include: user name, e-mail, address, telephone number, text of the advertisement, attached image or video recording, which may include the image or voice of the data subject.
(8) Duration of processing: the personal data are processed primarily until the deletion of the advertisement or, secondarily, until its withdrawal by the data subject. The data processing shall also cease upon deletion of the user account.

6.

(1) Online, electronic contracting on the Company's website (use of the online marketplace provided by the Data Controller) is subject to Act CVIII of 2001 (Eker Act). The content and terms of the electronic contract are set out in the GTC on the website. Personal data is required for the performance of the contract (GTC). If you do not provide us with this personal data, we will not be able to conclude a contract (GTC) with you and to perform the terms of the contract (GTC). The Privacy Policy and any annexes thereto are not contractual terms and do not become part of the General Terms and Conditions ("GTC") as part of an electronic contract with a registered user. References to the TOS shall at all times be construed as information relating to the processing of data and never as clauses forming part of the TOS.
(2) The purposes of the processing of data in connection with the use of the Service on the website:
- to identify and contact the seller and the buyer
- to identify and contact the seller and to establish contact with the seller
- to detect suspicious transactions during online payments
- proving compliance with the legal obligation to provide information to consumers
- proving the conclusion of a contract between the Data Controller and the user
- the creation, definition, modification and monitoring of the performance of the contract.

(3) In the case of the use by the user of the services provided by the Data Controller on the website, the legal basis for processing is (also) the consent of the data subject, the fulfillment of the contract and legal obligations and, in the case of the detection of abusive transactions, legitimate interest.
(4) The categories of data concerned by the processing are: the name, address, telephone number, e-mail address, access password, tax number of the user, images of products uploaded by the user, correspondence between the parties in the messaging system.
(5) Categories of persons concerned by the processing: any natural person who, as a registered user of the Controller's website, makes use of the services offered by the Controller.
(6) Categories of data recipients: the manager of the Data Controller; employees performing customer relations and sales-related tasks; employees of the Data Controller who operate the websites of the Data Controller, employees of the data processor who operate the websites of the Data Controller; employees of the Data Controller who perform accounting and invoicing tasks, employees of the data processor who perform these tasks; and employees of Verotel International B. V. (website: https://www.verotel.com/; e-mail: payments@verotel.com; telephone: + 00-800-44229999)
(7) Duration of data processing:
- Until 5 years after the performance of the contract, failing which until 5 years after the conclusion of the contract;
- If the Data Controller is obliged to keep the data under the Accounting Act, the Data Controller shall keep the data for 8 years after the purchase.

7. Messaging system

(1) The Data Controller shall provide a messaging system to registered data subjects with a user account for the communication of data subjects in connection with the sale of products on the website. The personal data and attachments provided in the message sent in the messaging system shall also be stored, and the Data Controller shall therefore also be entitled to process the data in the messaging system pursuant to this point.
(2) The legal basis for the processing of the data by the Controller in connection with the operation of the messaging system is the establishment and performance of a contractual relationship to which the data subject is a party.
(3) The data subject is any natural person who is registered on the website as required to use the messaging system and who uses the messaging system to exchange messages.
(5) The purposes of the processing: to maintain contact; to ensure secure communication between the parties concerned and to enable the identification of the other party in order to facilitate product sales.
(6) Recipients of personal data: the Data Controller's manager, employees performing customer service and marketing tasks on the basis of their job function and data processors performing tasks in this context, employees of the data processor performing tasks related to the operation of the Data Controller's website and related tasks.
(7) Personal data processed: user name, ad identifier, ad content, conversation id of messages, message identifier, message date, personal data (including image and sound recordings) contained in the message and attachments.
(8) Duration of processing: personal data are processed primarily until the deletion of the user account and secondarily until the withdrawal of the data subject's consent.

(8) Marketing

(1) The legal basis for the processing of data for marketing purposes by the Controller is the consent of the data subject, which is unambiguous, explicit and prior. The data subject shall give his or her unambiguous, explicit and prior consent by ticking the box next to the text "consent to marketing communications" on the Controller's website following the information concerning the processing of his or her data.
(2) The Controller may also process data for marketing purposes by means of cookies for marketing purposes, the provisions of which are set out in point 2 of this Notice.

(3) The data subject may also give his or her consent on paper by filling in a data form in a separate document.
(4) The data subject is any natural person who gives his or her unambiguous, explicit consent to the processing of his or her personal data by the Controller for marketing purposes.
(5) The purposes of the processing: keeping in contact; sending advertisements and offers related to the provision of services and the sale of products; sending notifications of promotions by electronic means or by post.
(6) Recipients of personal data: the Data Controller's manager, employees performing customer service and marketing tasks on the basis of their job function and data processors performing tasks in this context, employees of the data processor performing tasks related to the operation of the Data Controller's website.
(7) Personal data processed: name, address, telephone number, e-mail address.
(8) Duration of the processing: until the processing of personal data for marketing purposes is withdrawn by the data subject.

(9) Who has access to the personal data (recipients)

In general, for the processing operations referred to in this Notice, access to personal data shall be limited to the persons authorized by the Controller. In this Notice, the Controller has indicated for each type of processing the categories of persons to whom it may give authorisation. This means that the previously designated persons may have access to the personal data for the performance of their tasks.

The Data Controller also uses the web analytics services of Google LLC, 1600 Amphitheatre Parkway Mountain View CA 94043, Google Analytics, Google Adwords, a data protection shield in the EU-U.S., and Facebook Ireland Ltd.

The web analytics services also use cookies to help analyze the use of online interfaces. By providing specific and explicit consent to the use of the online interfaces, the data subject authorizes Google Analytics and Google Adwords to transfer information generated by cookies about the use of the online interface to Google servers in the United States of America. The other cookies processed are stored on servers within the European Union. By providing specific consent on the website, the user consents to the collection and analysis of his/her data in the manner and for the purposes set out above. The above-mentioned service providers use this information to evaluate and analyze the use of online interfaces by the data subject, to compile reports on the activities carried out on online interfaces and to provide other services related to the activities carried out on those interfaces and to the use of the Internet. However, it remains important to stress that the cookies used on the website do not store personally identifiable information.

The website even uses the following cookies, which do not transmit any data, but are exclusively cookies developed by the data controller itself, if the user ticks a box to stay logged in at the time of logging in, the cookie will monitor the user's activity for 1 week, while if the user does not tick it, it will only monitor the user's activity for 4 hours. The following cookies are essential for the website to work.

pinky-stories.prod.authToken
_pinky-stories.prod.authToken

10.

In connection with the online sale and purchase of products via the website, as a data processing objective, data relating to purchases made on the Internet will be transmitted to Verotel International B.V. (website: https://www.verotel.com/; e-mail: payments@verotel.com; telephone: +

00-800-44229999) in order to enable the company to process online card transactions securely and traceably via its network. This company guarantees the security of the personal data and the processing of the transaction through its own site (secure payment gateway, secure card payment guarantee window) when the card is used for payment after the purchase.

The data transmitted include: name, e-mail address, telephone number, address, billing address if different, IP address, other data related to the payment transaction.

The Data Controller's messaging system is provided by the Data Controller, so the messages and the related personal data are stored by the Data Controller.

The data transmitted includes: user name, e-mail address, telephone number, conversation id of messages, message ID, message date, personal data (including images and audio recordings) contained in the message and attachments.

## 11 Final provisions

The provisions of the Policy and its annexes shall apply to the data processing provisions not mentioned in this Policy, as stated at the beginning of this Policy. Thus, in particular, but not exclusively, the provisions of the Policy shall govern the rights of data subjects, data security measures and remedies.

November 2, 2023

Hugo Soft Limited Liability Company