PRIVACY POLICY

I. Introduction

The White Elephant Digital Ltd. (headquarters: 1093 Budapest, Lónyay utca 13/b. 3. emelet 26., company registration number: 01-09-335115, tax number: 26613152-2-43), as Data Controller shall act on the basis of this Privacy Policy (hereinafter: Policy) during the data management for the services provided by him, connected to using his Facebook and social media accounts, accepting his tender as well as any natural people entering into a contract with him (hereinafter: Data Subject). By expressly accepting the Policy, the Data Subject accepts the provisions of the current Policy as binding on himself.

The content of the current Policy is considered mandatory for the Data Controller and he states that this Policy complies with the current Hungarian legislation on data management and with the rules contained in the legal acts of the European Union.

The Data Controller reserves the right to unilaterally change this Policy at any time, which will be communicated in due time to the other party.

II. Aim of the Policy, Principles of Data Management

The purpose of this Policy is to determine the scope of personal data managed by the Data Controller, the way in which the data is handled, and to ensure the implementation of constitutional principles of data protection and data management, the implementation of information self-determination in order to ensure that the privacy of the natural persons of the Data Subject is respected, during the processing and handling of personal data.

The Data Controller acts in accordance with the requirements of good faith, fairness and transparency in co-operation with the Data Subjects during the data management. The Data Controller only manages the data specified by law or provided by the Data Subject for the purposes specified below. The scope of personal data handled is proportional to the purpose of the data management and cannot be extended beyond it.

The Data Controller does not check the personal data provided to him. Only the person providing it is responsible for the adequacy of the personal data provided.

The personal data of a person under the age of 16 may only be processed with the consent of an adult of parental authority. The Data Controller is not in a position to verify the eligibility of the content of the statement, so the Data Subject or the person exercising parental authority over it guarantees that the consent is in compliance with the law. In the absence of the consent, the Data Controller does not collect any personal data related to a person who has not reached the age of 16 years.

Considering the relevant provisions of the General Data Protection Regulation (hereinafter: GDPR), the Data Controller is not obliged to appoint a data controller officer, since the Data Controller is not a public authority, the activities of the Data Controller do not include any operations that require regular and systematic large-scale observations by the Data Subject and the Data Controller does not manage special data or personal data relating to criminal offenses.

The principles of data management are in accordance with the following legislation in force:

- Regulation no. 2016/679 of the European Parliament and Council (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 as well as the repealing of regulation 95/46/EK (General Data Protection Regulation)
- Act CXII of 2011 on information self-determination and freedom information (hereinafter: Information Act)
- Act V of 2013 on the Civil Code (hereinafter: Civil Code)
- Section 169 of Act C of 2000 on accounting (concerning the retention of documents).

III. Interpretative Provision

a, personal data: any information related to an identified or identifiable natural person ("Data Subject"), any information that identifies directly or indirectly a natural person, in particular any information related to person such as name, number, position data, online identifier or one or more factor relating to the physical, physiological, genetic, intellectual, economic, cultural or social identity of a natural person.

b, data processing: any set of operations or operations performed automated or non-automated on personal data or files, such as collection, recording, systematization, segregation, storage, transformation or alteration, query, insight, use, communication, transmission, distribution or any other way of making it available, coordination or interconnection, restriction, deletion or destruction.

c, data controller: any natural or legal person, public authority, agency or any other body which determines the purposes and means of processing of personal data, either alone or in association with others; if the purposes and means of data management are defined by EU or member state law, the specific aspects of the appointment of controller may be determined by the European Union or national law.

d, data processor: any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller.

e, the addressee: any natural or legal person, public authority, agency or any other body with which the personal data are communicated, whether or not they are third parties. Public authorities which have access to personal data in accordance with European Union or member state law in the context of a specific investigation shall not be considered as an addressee, the handling of such data by these public authorities must comply with the applicable data protection rules in accordance with the purposes of the data management.

f, third party: any natural or legal person, public authority, agency or any other body which is not the same as the data subject, controller, processor or the persons authorised to process personal data under the direct control of the controller or processor.

g, registration system: a set of personal data that is in any way – centralized, decentralized, functionally or geographically – accessible based on specified criteria.

h, data protection incident: a security breach that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access to personal data transmitted, stored or otherwise processed.

i, representative: any natural or legal person who has residence or activity site within the European Union, identified by the data controller or processor based on the Article 27 of GDPR, who represents the controller or the processor for the purposes of obligations under the GDPR.

j, enterprise: any natural or legal person pursuing an economic activity, regardless of its legal form, including partnerships and associations carrying out regular economic activities.

k, technical and organizational measures: a procedure to ensure and demonstrate that the processing of personal data is managed in accordance with the nature, scope, circumstances, and objectives of the data subject and taking into the risks to the rights and freedoms of natural persons, with varying degrees of probability and severity, in accordance with GDPR. These measures are reviewed and updated by the controller if necessary.

IV. Data Processor

The Data Controller may use a data processor authorized to perform its activities. Data Processors cannot make any independent decisions, they are only entitled to act upon the contract with the Data Controller and the instructions received. The Data Controller checks the work of the data processors. Data processors shall only be entitled to use other data processors with the consent of the Data Controller.

Data Processors used by the Data Controller:

Accounting:

- Full Active Bt Adatfeldolgozó és Szolgáltató Betéti Társaság (Headquarters: 1156 Budapest, Nyírpalota u. 74. 6. em. 26., Tax Number: 20797999-1-42, Company Registration Number: 01-06-737094, Representative: Nagy Zoltán)
- Szamlazz.hu - KBOSS.hu Kft. (Headquarters: 1031 Budapest, Záhony utca 7., Tax Number: 13421739-2-41, Company Registration Number: 01-09-303201, Representative: Ángyán Balázs)

IT:

- DOPAMA Informatikai Korlátolt Felelősségű Társaság (Headquarters: 1163 Budapest, Döbröce utca 45., Tax Number: 25064115-2-42, Company Registration Number: 01-09-197639, Representative: Dósa Zsolt)

Telephone service:

- Vodafone Magyarország Mobil Távközlési Zártkörűen Működő Részvénytársaság (Headquarters: 1096 Budapest, Lechner Ödön fasor 6., Tax Number: 11895927-2-44, Company Registration Number: 01-10-044159, Representative: Amanda Nelson)

Hosting provider:

- Google LLC (Corporate Headquarters: 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA) European Economic Area or Switzerland: Headquarters: Google Ireland Limited (Gordon House, Barrow Street, Dublin 4, Ireland)
- Trello (Atlassian Corporation Plc., Headquarters: Sydney, Australia, Level 6 341 George Street)

- Webonic Kft. (Headquarters: 8000 Székesfehérvár, Budai út 9-11., Company Registration Number: 07-09-025725, Tax Number: 25138205-2-07, Representative: Michal Truban)

Newsletter:

- Mailchimp (The Rocket Science Group LLC, Headquarters: 675 Ponce de Leon Avenue NE Suite 5000, Atlanta, GA 30308, United States)

In addition to the above, personal data relating to the data subject may be transmitted only in the cases specified by law or on the basis of consent from the data subject, in which case the Data Controller shall obtain the explicit consent of the data subject prior to the commencement of the transfer of personal data related to him or her.

V. The scope of managed personal data

1. Job applicants
   a) Scope: any natural person applying for a job application posted by the Data Controller
   b) Scope of data:
      - Name
      - Email address
      - Phone number
      - Photo
      - Age
      - Education
      - Previous work places
      - Occasionally references
   c) Aim of data management: identifying the person, investigation of professional qualities, keeping in touch
   d) Legal basis for data management: the consent of the data subject, with written statement (via the Data Controller's website or Facebook page) that he or she accepts and allows the management of personal data on the basis of this Policy.
   e) Source of data: personal data voluntarily provided by the data subject
   f) Duration of data management: until the aim is reached, or on the basis of the data subject's consent, up to a maximum of 6 months after the application, or until cancellation requested by the data subject in the meantime.
   g) Data management process: the data subject submits the application containing personal data to the Data Controller, typically through email via the Data Controller's website or Facebook page. During the selection process, the Data Controller compares the applications with conditions for establishing the employment/other legal relationship based on the position, and on the basis of comparison, invites the most suitable people for a personal interview. The selection process continues with the personal interview and, if necessary, with the completion of a test.

If a reference person has been designated by the applicant, the Data Controller may contact that person to verify the professional experience of the data subject.

The selection ends with the conclusion of a contract with the most relevant applicant, with the comment that the Data Controller can only manage the data of unelected parties if it has been specifically agreed to by the data subjects in a separate, verifiable manner.

The Data Controller indicates the results of the selection to the affected applicants and requests the consent for data management for the same or similar job applications or for the

same or similar required qualities for a further period of up to 6 months after the application, if no such contribution was previously provided by the data subject. The data Controller attaches the consent to the data and stores it.

2. Management of employee data
   a) Scope: any natural person who establishes an employment relationship or other legal relationship with the Data Controller for which the Data Controller has a reporting obligation.
   b) Scope of data:

In case of employment relationship:

- Family name and first name
- Place of birth
- Date of birth
- Mother's name
- Home address
- Tax identification number
- Social security number
- Qualifications and the institution issuing the document certifying it
- FEOR number
- Beginning, code and termination of health insurance
- Duration of break in health insurance
- Weekly working hours
- Gross personal wages
- Net personal wages
- Bank account number
- ID card number
- Phone number
- Email address
- Photo of the person
- Knowledge of foreign language
- Job, job description
- Management assignments
- Internship time, exam, probation
- Disciplinary proceedings, punishment, relief
- Criminal record
- Level of payment
- Scientific research (publication)
- Artistic creative activity
- Working time
- Workable time
- Classification information
- Honors, awards and other received prizes

In case of simple employment:

- Family and first name
- Place of birth
- Date of birth
- Mother's name
- Home address

- Tax identification number
- Social security number
- Nature of simplified work
- Job title
- Start and end date of employment
- Number of hours worked per day for casual work
- Working hours
- Gross basic salary
- Net basic salary
- Bank account number
- Place of work

In case of engagement contract:

- Family and first name
- Place of birth
- Date of birth
- Mother's name
- Home address
- Tax identification number
- Social security number
- Start of contract
- FEOR number
- Beginning, code and termination of health insurance
- Duration of break in health insurance
- Weekly working hours
- Gross commission fee
- Net commission fee
- Bank account number
- Place of work

c) Aim of data management: fulfilment of legal obligations
d) Legal basis for data management: based on voluntary consent, but data management is mandatory based on the Annex 1 of Act CL of 2011 and ACT 3 and 11 of LXXV of 2010 on simplified employment.
e) Source of data: personal data voluntarily provided by the data subject
f) Duration of data management: storing the data for 5 years from the end of the calendar year of staff member's exit, with prohibition of scrapping labor, wage and social security records
g) Data management process: The Data Controller informs the Data Subject that he has a statutory reporting obligation to the tax and customs authorities in respect of the data to be provided, which is acknowledged in writing by the data subject. In case the data subject does not wish to acknowledge the fulfilment of the legal obligations, or does not consent to them, no employment relationship, simplified employment or engagement contract can be established. After acknowledgement, the data subject, future Employee establishes an employment relationship, simplified employment or engagement contract with the Data Controller, by entering into a relevant contract, which the Data Controller stores. In order to fulfil its statutory obligations, the Data Controller shall disclose the data to be provided by communicating his/her own tax number, name, headquarter address, location, name and tax number of legal predecessors, to the competent state

tax and custom boards by electronic means or on a provided form, transferring the data this way.

3. Potential customers
   a) Scope: any natural person who establishes a relationship with the Data Controller at meetings, conferences, the Data Controller's website, or any other request for possible future co-operation with the Data Controller
   b) Scope of data:
      - Name
      - Email address
      - Phone number
      - Company
      - Position
      - Address of the company
   c) Aim of data management: Identification of the concerned and the company he/she represents, professional communication for future cooperation, personal contact
   d) Legal basis for data management: voluntary consent of the data subject, with the written consent of the data subject (website, professional events on a paper basis), that he/she accepts and consents to the management of personal information, based on this current Policy
   e) Source of data: personal data voluntarily provided by the data subject
   f) Duration of data management: until the purpose of data management has ceased, so in the future the Data Controller does not intend to establish a professional relationship with the data subject or the organization he/she represents, or until a cancellation request is made in the meantime
   g) Data management process: the Data Controller can get to know the data subject at professional meetings, conferences, where he gives his name and contact details on paper and occasionally, which organization he represents at the event. The data subject may also contact the Data Controller through his website, where he can enter his contact details on the contact detail form provided by the Data Controller. The Data Controller may, on the basis of the data provided by the data subject, contact the data subject or the represented organization, in order to establish a professional relationship or a contractual relationship.

4. Contracting clients

a) Scope: any natural persons or natural persons acting on behalf of an organization, who establishes an agreement with the Data Controller (in addition to providing personal data) to use the Data Controller's services

b) Scope of data:

- name

- phone number

- email address

- subject of service

- remuneration

c) aim of data management: identification of client, providing services to the client in accordance with the provisions of the agreement, keeping in contact

d) legal basis of data management: voluntary consent of the data subject, in a written form (within the contract established with the Data Controller) that he/she agrees and constants to the management of personal data in order to fulfil the contract, in accordance with this Privacy Policy

e) source of data: personal data voluntarily provided by the data subject

f) duration of data management: it shall expire on the expiry of the rights and obligations arising from the legal relationship with which the Data Controller handles personal data, with regard to data that are supported by supporting documents and supporting the accounting records, under Section 169 (2) of Law C of 2000, at least for 8 years.

g) data management process: the data subject informs the Data Controller of the acceptance of the Data Controller's offer in a manner provided by the Data Controller and accessible by the data subject. The Data Controller will work out the details of the service agreement with the affected person, taking into account the content of the accepted offer. The data subject gives his/her data to the Data Controller voluntarily and without influence, and then concludes the agreement with the Data Controller. The Data Controller records the agreement in electronic and/or paper-based form in a filing system. The Data Controller can inform the data subject about each step in the execution process. The data subject, in accordance with the purpose of the data management, voluntarily agrees to contact the Data Controller through his/her contact details regarding the reconciliation of the details of the performance and/or related issues.

5. Newsletter

a) Scope: any natural person who wishes to be regularly informed about news, promotions, events of the Data Controller by providing his/her personal data to subscribe to the newsletter service

b) scope of data:

- name

- email address

c) Aim of data management: informing about new or renewed services, advertisement-based content for marketing or sales purposes, customer satisfaction measurement, invitation for marketing event

d) legal basis for data management: voluntary consent of the data subject, in a written form (by subscribing to the newsletter) that he/she agrees and constants to the management of personal data, in accordance with this Privacy Policy

e) source of data: personal data voluntarily provided by the data subject

f) duration of data management: until the data subject unsubscribes through the marketing@whiteelephant.digital email address

g) data management process: The data subject may subscribe to the newsletter via the Data Controller's website, on the basis of which the Data Controller periodically sends a newsletter to the data subject. The Data Controller reviews the subscriber database every 3 years and after 3 years asks for a new consent from the subscribers. If the data subject does not give consent, the Data Controller will delete its data.

6. Presence and marketing on social media sites

a) scope: any natural persons who voluntarily follow, share, prefer to share the social media pages of the Data Controller, in particular on Facebook, Instagram, LinkedIn, Twitter site, or content appearing on them.

b) scope of data:

- public name

- public photo

- public email address

- message sent through public social media sites

- the result of an evaluation by the person or any other operation

c) aim of data management: The purpose of the presence on social media sites and the related data management is to share, publish and market the content on the website. With the help of social media channels, the people can get information about the latest news, events and launches.

d) legal basis for data management: voluntary consent of the data subject, by following and liking the content of the Data Controller on social media sites

e) source of data: personal data voluntarily provided by the data subject

f) duration of data management: until the request of cancellation by the data subject

g) data management process: The Data Controller communicates with the data subject parties via the social network only if the data subject reaches out to the Data Controller through social media, hereby making the aim of data management relevant. The Data Controller can link other social media pages together, based on the specific platform's regulations, this should include the publication of content on linked social media pages too. If it is not a recording of a crowd or public performances, based on Civil Code 2:48, the Data Controller always requests the written consent of the data subject prior to the publication of the images. The data subject may request additional information regarding data processing and management on the specific social media platform.

7. Billing

a) Scope: any natural person or any natural person acting on behalf of an organization who, with the provision of personal data. concludes an agreement with the Data Controller in order to request the services of the Data Controller and pays a fee to the Data Controller at specified intervals

b) scope of data:

- name

- address

- phone number

- email address

- tax identification number

c) aim of data management: issue of an accounting document about the fees of services provided by the Data Controller, in accordance with the conditions set out in Law C of 2000

d) legal basis of data management: voluntary consent of the data subject, in a written form (within the contract established with the Data Controller) the data subject accepts and agrees to the management of personal data, a legitimate interest for the performance of the contract

e) source of data: personal data voluntarily provided by the data subject

f) duration of data management: on the basis of Law C of 2000, 169:2, for at least 8 years.

g) data management process: the data subject provides in the contract with the Data Controller the data required for the accounting document to be issued and the contact details through which the Data Controller can forward the accounting document. The Data Controller shall forward the accounting document to the data subject to the contact details provided by the data subject for a specified period of time.

VI. Deleting the Data

The Data Controller deletes personal data if

a) it is handled unlawfully: if the data is found to be unlawfully processed, the Data Controller shall promptly execute the deletion.
b) the data subject requests it (except data processing based on law): the data subject may request the deletion of data on the basis of the voluntary consent of the data subject. In this case, the Data Controller deletes the data. The cancellation can only be denied if the law authorizes the processing of the data. In all cases, the Data Controller shall provide information on the refusal of the cancellation request and on the legislation permitting the processing of data.
c) the data is incomplete or incorrect – and this condition cannot be remedied legally – provided that the cancellation is not excluded by law
d) the purpose of the data management has ceased to exist or the statutory time limit for storing the data has expired
e) it has been ordered by the National Authority for Data Protection and Freedom of Information. If the court or the Authority has ordered the deletion of the data, the Data Controller shall execute the deletion.

The deletion can be denied:

- to exercise the right to freedom of expression and information
- when authorized to handle personal data by law and legal claims.

In any case, the Data Controller shall inform the data subject of the refusal of the cancellation request, indicating the reason for the refusal to cancel. Once the request for deletion of personal data has been completed, the previous (deleted) data cannot be recovered.

All other data will be deleted by the Data Controller if it is obvious that the data will not be used in the future, i.e. the purpose of the data management has ceased.

Instead of deletion, the Data Controller - in addition to informing the data subject - locks the personal data if requested by the data subject or if based on the available information it can be assumed that the deletion would violate the legitimate interests of the data subject. The personal data

blocked in this way can only be processed until the data management purpose that excludes the deletion of the personal data exists. The Data Controller identifies the personal data he / she manages if the data subject disputes its accuracy, but the inaccuracy of the personal data at issue cannot be clearly established.

In the case of data processing ordered by law, the deletion of data is governed by the law.

In case of deletion, the Data Controller makes the data unsuitable for personal identification. If required by law, the Data Controller will destroy the media containing the personal data.

VII. **Data Security**

The Data Controller shall ensure the security of the data, take the technical and organizational measures and establish the procedural rules necessary for the enforcement of the applicable laws, data and confidentiality rules. The Data Controller protects the data with appropriate measures against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as against unavailability due to accidental destruction and damage to the technology used.

The Data Controller shall keep records of the data it manages in accordance with the applicable legislation, ensuring that the data is only accessible to those employees and other persons (data processors) acting in the Data Controller's interest who are required to perform their duties. Data can only be found in the employee's organization by logging. The Data Controller's employees perform individual searches, individual operations on the data only at the request of the data subject, or in case it is necessary for the provision of the service.

Data Controller keeps records of his contracts on paper, as well as invoices received by post, and pay roll papers that are stored in a lockable cabinet, which is only accessible to the company's manager.

The data manager stores all other data electronically in the storage space provided by the hosting service providers and on his own server.

The Data Controller takes into account the state of the art of technology in determining and applying data security measures. The Data Controller chooses one out of the several possible data management solutions that provides the highest level of protection for personal data, unless it would be a disproportionate difficulty.

In particular, the following are included in the Data Controller's tasks connected to data IT security:

- measures to protect against unauthorized access, including protection of software and hardware devices, and physical protection
- measures to ensure the recovery of data files, including regular backups and separate, secure handling of copies
- protection of data files against viruses
- physical protection of data files and devices carrying them, including protection against fire damage, water damage, lightning strikes, other elementary damage, and recoverability of damage resulting from such events.

Employees and other persons acting in the interest of the Data Controller are obliged to safely preserve and protect unauthorized access, alteration, transmission, disclosure, deletion or disclosure

of data media used by them or in their possession, including personal data, irrespective of how the data are recorded.

The Data Controller operates the electronic register through an IT program that meets the data security requirements. The program ensures that only those people who need it for the purpose of performing their duties can access the data only for targeted purposes, under controlled conditions.

VIII. **Rights of Data Subjects**

The following rights are available to the data subject as affected party:

a) The right for information: The Data Controller provides a concise, transparent, understandable and easily accessible form of information to the Data Subject in a clear and comprehensible manner. The Data Subject can exercise this right in writing through the points detailed in this Policy's VIII/2 and shall be informed by the Data Controller.

b) The right for access: The Data Subject shall have the right to receive feedback from the Data Controller on whether personal data are being processed and, if such data is being processed, to have access to the personal data and information listed in the regulation.

c) The right of rectification: The Data Subject shall have the right, at his request, to correct the inaccurate personal data relating to him or to supplement the incomplete personal data without undue delay.

d) The right for deletion: The Data Subject shall be entitled for deletion of personal data upon request to the Data Controller without undue delay, and the Data Controller shall be obliged to delete the personal data concerning the Subject without undue delay under the conditions specified below:

- personal data are no longer needed for the purpose for which they were collected or otherwise processed;
- the Data Subject withdraws the consent of the data management, and the data management has no other legal basis;
- the Data Subject has objected to the data management and there is no legitimate legal reason for data management;
- unlawful processing of personal data;
- the personal data must be erased in order to fulfill a legal obligation under EU or Member State law applicable to the controller;
- the collection of personal data related to the provision of information society services.

e) The right to be forgotten: If the Data Controller has disclosed personal data and is obliged to delete it, it will take reasonable steps, including technical measures, to take into account the cost of the technology and implementation, in order to inform data processors managing the data that the Data Subject has requested the personal information's links and copies in question to be deleted and erased.

f) Restriction of Rights for Data Processing

The Data Subject has the right to request the Controller to restrict the processing if one of the conditions below is met:

- the Data Subject debates the accuracy of personal data. In this case the restriction is pertained for the time period until the Controller is able to verify the accuracy of personal data;
- processing is illicit, and the Data Subject is against the deletion of data, and requests the limitation of their use instead;
- the Controller does not need the personal data for processing anymore, but the Data Subject needs them for the establishment, exercise or defence of legal claims;
- the Data Subject objected to their data being processed; in this case the restriction is pertained for the time period until it is stated if the legitimate reasons of the Controller prevail over the legitimate reasons of the Data Subject.

If the data processing is subject to restrictions, personal data should only be stored, and processed only with the consent of the Data Subject, or for the establishment, exercise or defence of legal claims, or to defend the rights of other natural or legal persons, or if it is the important public interest of the Union or one of its member states.

The Controller informs the Data Subject before lifting the restrictions on processing.

g) Right to data portability: the Data Subject shall have the right to receive the personal data concerning them, which they have provided to the Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.

h) Right to object: The Data Subject shall have the right to object at any time, on grounds relating to their particular situation, to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller, or the purposes of the legitimate interests pursued by a controller or by a third party, including profiling based on the aforementioned provisions. In this case, the Controller shall 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 defence of legal claims.

If 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 them for such purposes, including profiling, if it is related to direct marketing.

If the Data Subject objects to the processing for direct marketing purposes, the personal data is no longer allowed to be processed for such purposes.

i) Automated individual decision-making, including profiling: the Data Subject is entitled to be excluded from the scope of decisions based exclusively on automated processing including profiling that may produce legal effects regarding them, or may affect them similarly significantly.

The aforementioned entitlement shall not apply in cases when the decision:

- is necessary for entering into, or performance of, a contract between the Data Subject and the Controller
- is authorised by Union or Member State law to which the controller is subject to and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests; or

- is based on the explicit consent of the Data Subject.

j) Right of withdrawal: The Data Subject shall have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

1. The Controller informs the Data Subject about any measure taken based on the request in accordance with the aforementioned rights without any unsubstantiated delay, but in any event within a 1-month deadline. Considering the complexity and the number of requests, this deadline can be prolonged with further 2 months if needed. The Controller informs the Data Subject about the prolongation of this deadline, and sets out the reasons for the delay within 1 month of receipt of the request at the latest. If the Data Subject issued the request in an electronic way, the information shall be given in an electronic way, unless requested by the data subject otherwise. If the Controller does not take action on the request of the Data Subject, the Controller shall inform the Data Subject without delay and at the latest within 1 month of receipt of the request, stating the reasons for not taking action, and informing the Data Subject about their right to lodge a complaint with a supervisory authority and seek judicial remedy.

The Controller shall provide the requested information, communication and provision free of charge. If the request of the Data Subject is proven to be unfounded, or excessive, particularly because of their repetitive character, the Controller may:

a, charge a reasonable fee for the administrative costs for providing the information or the communication or taking the action requested

b, may refuse to act on the request.

The Controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

The Controller informs all addressees with whom the personal data have been shared about every correction, deletion or restriction of processing done by the Controller, unless this proves to be impossible or involves disproportionate effort. The Data Subject may request to be informed about these addressees by the Controller.

The Controller makes the copy of the personal data undergoing processing available for the Data Subject. The Controller may charge a reasonable fee for the administrative costs of further copies requested by the Data Subject. If the Data Subject issued the request in an electronic way, the information shall be given in a commonly used electronic format, unless the Data Subject requests otherwise.

2. The Data Subject may contact the Controller about questions and observations concerning data processing at:

- email: finance@whiteelephant.digital
- mailing address: 1093 Budapest, Lónyay utca 13/b 3. emelet 26.

3. If their rights are violated, the Data Subject may go to court against the Controller. In this case, the court acts through an expeditious procedure.

4. All complaints shall be made to the Hungarian National Authority for Data Protection and Freedom of Information.

Hungarian National Authority for Data Protection and Freedom of Information
Seat: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Mailing address: 1530 Budapest, Pf. 5.
Phone: 06-1-391-1400
Fax: 06-1-391-1410
E-mail: ugyfelszolgalat@naih.hu
Website: http://www.naih.hu

IX. TASKS CONCERNING DATA PROCESSING

The Controller prepares and sends newsletters to the clients of its contractors ('The Partner') for different purposes (reminders, advertisements, events, etc.).

The legal basis for data processing is based on an agreement.

Those subject to data processing: clients of The Partner, natural persons subscribing to the newsletter of The Partner.

Data subject to data processing and the goal of data processing carried out by the Controller regarding clients of The Partner:
- name
- email address

Goal of data processing: sending newsletters by The Partner, for clients of The Partner.
Time scope of data processing: not more than 12 months from the date of termination of contractual relationship with the counterparty.

X. OTHER PROVISIONS

In every case when the Controller intends to use the provided data for purposes other than the original purpose of data collection, the Controller shall inform the Data Subject, obtain their explicit prior consent and provide opportunity for them to forbid the use of data.

The Controller is obliged to ensure the security of the data, and to take technical measures to ensure that the recorded, stored and managed data are protected, and to do its best to prevent their destruction, unauthorized use and unauthorized alteration. The Controller is also obliged to call every third party to whom these data are forwarded or handed to for the fulfilment of their obligations in this regard.

Dated.: Budapest, 01. 01. 2019.

White Elephant Digital Kft.
Sztaniszláv András executive director