ELEKTRO PROFI VÁLLALKOZÁSI KFT.

Data management information

Az ELEKTRO PROFI Vállalkozási Kft. (1148 Budapest, Fogarasi road 2-6.) data controller issues the following data management policy and information for its customers, other business parties, visitors to the website www.elektroprofi.eu, as well as for other personal data processing:

As a data controller, ELEKTRO PROFI Vállalkozási Kft. accepts the content of this policy binding for itself, whereby it takes particular care to the protection of personal data. ELEKTRO PROFI Vállalkozási Kft. performs data processing in compliance with the applicable Hungarian data protection law, Regulation 2016/679 of the European Parliament (EU) and Council (GDPR decree) and the provisions of these Rules.
The current data management policy of ELEKTRO PROFI Vállalkozási Kft. is constantly available at http://www.elektroprofi.eu/.
ELEKTRO PROFI Vállalkozási Kft. reserves the right to change this information at any time, of which it informs the data subjects in a timely manner.
If any provision contained in these Rules is not clear to a person, ELEKTRO PROFI Vállalkozási Kft. is ready to help in the interpretation of the provisions of the Rules.
ELEKTRO PROFI Vállalkozási Ltd. is committed to protecting the personal data of its users and partners and respecting the right of informational self-determination of its clients is of paramount importance. ELEKTRO PROFI Vállalkozási Kft. treats personal data confidentially and takes all security, technical and organizational measures that guarantee the security of the data.
ELEKTRO PROFI Vállalkozási Ltd. describes its data management principles herein and presents the expectations that it has defined and it adheres to them as a data controller.

Data of the hosting provider:

Name: NEXTSERVER Kft.
Registered seat: 6722 Szeged, Mérey Street 12
Tax number: 22797610-2-06
Phone number: 06 1 445 1300
E-mail: info@nextserver.hu

1. **Legislation on which data processing is based:**

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46 general data protection regulation).
- - Act 112 of 2011 on Information Self-Determination and Freedom of Information,
- - Act 5 of 2013 on the Civil Code,

- Act 66 of 1995 on the protection of Public Documents, Public and f Private Archives.
- Act 108 of 2001 on certain aspects of electronic commerce services and information society services

- Act 100 of 2003 on Electronic Communications.

Pursuant to Section (1) of § 20 of Act 112 of 2011 on Informational Self-Determination and Freedom of Information (Info tv.), ELEKTRO PROFI Vállalkozási Kft. informs the data subject (hereinafter referred to as "user or person") prior to the start of data processing that the data processing is based on consent or it is mandatory.

Before starting the processing, the data subject shall be clearly and in details be informed of all facts relating to the processing of his data, in particular the **purpose and legal basis of the processing, the person entitled to process and the duration of data processing**.

The Info TV. Pursuant to Article (1) of § 6, the data subject must also be informed that personal data can be processed even if obtaining the consent of the data subject would be impossible or it would involve disproportionate costs, and the processing of personal data is needed for the purposes of fulfilling the legal obligation of the controller for the legitimate interest of the controller or third party, and the enforcement of that interest is proportionate to the restriction of the right to the protection of personal data.

The information shall also cover the rights and remedies of the data subject in relation to data processing.

If personal information to data subjects would be impossible or would involve disproportionate costs (such as at a website), the information may also be provided by disclosing the following information:

(a) the fact of data collection,
(b) the scope of data subjects,
(c) the purpose of the data collection,
d) the duration of the processing,
(e) the identity of potential controllers entitled to access the data,
(f) a description of the rights and remedies of data subjects in relation to data processing, and
g) where data processing is subject to data protection registration, the registration number of the processing.

1.1. Personal data can therefore be processed if the data subject expressly agrees to it or orders it for public interest purposes by law or by decree of the local government on the basis of the authority of the law and within the scope specified therein.

1.2. Personal data may be processed even if obtaining the consent of the data subject is impossible or it would involve disproportionate costs and the processing of personal data

(a) is necessary for the purpose of fulfilling a legal obligation for the controller, or
(b) is necessary for the purposes of pursuing the legitimate interest of the controller or third party and the enforcement of that interest is proportionate to the limitation of the right to the protection of personal data.

1.3. If the data subject is unable to give his consent because of his incapacity or for other unavoidable reasons, then the personal data of the data subject may be processed during the existence of obstacles to consent for the protection of his or her or others' vital interests and prevention or avoidance of an imminent threat to the life, physical integrity or property of persons to the extent necessary, .

1.4. The validity of a legal statement containing the consent of a minor who has reached the age of 16 does not require the consent or subsequent approval of his/her legal representative.

1.5. If the purpose of data management based on consent is implementation of the contract concluded with the data controller in writing, then the contract must include any information that must be familiar for the concerned,; in particular definition of the data to be managed, duration of data management, purpose of use, fact, addressees of data transfer, the fact of employing the data controller. The contract must clearly state that the concerned person gives his/her consent to the management of his/her data as determined in the contract.

1.6. If the personal data were collected with the consent of the data subject, the data controller shall, unless otherwise provided by law, use the data collected for the purpose of fulfilling the legal obligation or for the purpose of enforcing the legitimate interest of the controller or third party, if the enforcement of such interest is proportionate to the restriction of the right to the protection of personal data

This Information and any amendments thereto shall take effect upon publication at www.elektroprofi.eu .

2. Interpretations of terms and concepts used in this Data Management information;

1. Concerned person/user: any specific natural person identified directly or indirectly, identifiable on the basis of personal data;
2. personal data: the data relating to the data subject, in particular the name, identification, one or more physical, physiological, mental, economic, cultural or social features of the data subject, and the conclusion drawn from the data as to the concerned person;
3. Specific information:
a) personal data relating to race, origin, nationality, political opinion or party status, religious or other philosophical beliefs, membership in representative organisation, sexual attitude,
(b) personal data on health status, abnormal passion and criminal affairs;
4. contribution: a voluntary and firm statement of the will of the data subject, based on appropriate information and giving his unambiguous consent to the processing of personal data relating to him, either in full or in particular operations;
5. objection: a statement by the data subject meaning that he/she objects to the processing of his/her personal data and requests the cessation of processing or the erasure of the processed data;
6. controller: a natural or legal person, or an organisation without legal entity, which alone or jointly with others determines the purpose for which the data are processed, makes and executes decisions relating to the processing (including the means used), or have it carried out by a processor entrusted to it;
7. data management: a set of operations carried out on the data irrespective of the procedure used, in particular the collection, recording, entering, organisation, storage, alteration, use, query, transmission, disclosure, coordination, or linking, blocking, erasing and destroying, preventing the reuse of data, taking photographs, sound or images, and recording physical characteristics (e.g. fingerprints, palmprints, DNA samples, iris images) that can identify the person;
8. data transfer: making the data accessible for a definite third party;
9. disclosure: making the data available for anybody;

10. data deletion: making data unrecognizable in such a way that its recovery is no longer possible;
11. data designation: the identification marking of the data for the purpose of distinguishing it;
12. data blocking: giving an identification to the data, for the purpose of limiting further processing thereof forever or for a specified period of time;
13. data destruction: total physical destruction of the media containing the data;
14. data processing: the performance of technical tasks relating to data processing operations, irrespective of the method and means used to carry out operations and the place of application, provided that the technical task is carried out on the data;
15. processor: any natural or legal person or organisation without legal personality who processes data on the basis of a contract concluded with the controller, including the conclusion of contracts under the provision of law;
16. data controller: the body with a public service mission which produced data of public interest to be published by electronic means or in the course of which this data was generated;
17. informant: a body with a public service mission which, if the data controller does not publish the data itself, publishes the data transmitted to it by the data controller on a website;
18. data file: complex of data managed in one record
19 “data protection incident”: a breach of security which entails accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed.
20. third party means a natural or legal person, or an entity without legal personality, other than the data subject, the controller or the processor;

3. Purpose limitation of data management

1. Personal data shall be processed only for specific purposes, for the exercise of rights and for fulfilment of obligations. At all stages of data processing it must correspond to the purpose of the processing, the collection and processing of data must be fair and legal.

2. Only personal data that is essential to the fulfilment of the purpose of the data processing and suitable for the purpose can be processed. Personal data can only be processed to the extent and for the time necessary to achieve the purpose.

4. Other principles of data management

The personal data retains its quality during the processing as long as its relationship with the data subject can be restored. The relation with the data subject can be restored if the controller has the technical conditions necessary for restoration. The processing shall ensure that the data subject can only be identified for the period necessary for the purposes of the processing.

5. Technical data

5.1. Data of the Data Subject's login computer that is generated during the use of the service and which are recorded by the Service Provider's system as an automatic result of technical processes. These are, in particular, the date and time of the visit, the IP address of the Data Subject's computer, the type of browser, the address of the visited and previously visited website.

5.2. The data recorded automatically shall be logged automatically at the time of entry or exit without a separate statement or action of the Data Subject. This data may

not be combined with other personal user data, except in cases required by law. Only the Service Provider shall have access to the data.

5.3. The Service Provider's system may collect data on the activity of the Data Subject, which cannot be connected with other data provided by the Data Subject, nor with data generated when using other websites or services.

5.4. The html code of the Website may contain links that are independent of the Service Provider from an external server and point to an external server. The service providers of these links are able to collect user data due to direct connection to their servers. External servers help to independently measure and audit the visitation and other web analytics data of the Website (Google Analytics). Data controllers can provide detailed information to the Data Subject on the handling of measurement data .

Contact details: www.google.com/analytics/

5.5. Service Provider may display Display ads to Data Subjects, on the Google Display Network and other online surfaces. Visitors can turn off data collection and change their settings using Ads Preferences Manager.

5.6. The Website may use Google Adwords's remarketing tracking codes. This is based on the opportunity to contact visitors later on Google Display websites with remarketing ads. The remarketing code uses cookies to tag visitors. Users of the Site may opt out of these cookies by visiting the Google Advertising Settings Manager and following the instructions provided therein. They will no longer receive personalized offers from the Service Provider.

6. Business Card Data Management

6.1. Legal basis of data processing: the User's voluntary consent, which is carried out by the act, when the User transfers the visit card containing his/her personal data to the Service Provider.

6.2. The scope of the data processed: name, telephone number, address, e-mail address, place of work and address, as well as other personal data on the visit card.

6.3. Purpose of data processing: building relationships, facilitating contact between persons.

6.4. The provisions of this data management policy shall be applied accordingly in the case of the transfer of visit cards and their handling.

6.5. Deadline for deletion of data: until the withdrawal of the consent statement, i.e. until the order to destroy the visit card.

6.6. Persons of the potential data controllers entitled to get the data: Personal data may be processed by the staff of the controller, respecting the above principles.

7. Data processing for employees

For these purposes, ELEKTRO PROFI Vállalkozási Kft. issues a separate data management policy.

8. Data Security

8.1. The controller shall design and implement the processing operations in such a way as to ensure the privacy of the data subjects.

8.2. The data controller or the data processor in his scope of activity is obliged to take care of data security, he/she is obliged to do the technical and organizational measures and develop the procedural rules required for the enforcement of info tv. and of the other data and secrecy protection rules.

8.3. The data shall be protected - with appropriate measures - against, in particular, unauthorized access, alteration, transfer, disclosure, deletion or destruction, as well as incidental liquidation and damage and becoming of inaccessible due to the change in the applied technics.

8.4. In order to protect the data filed electronically managed in the different records it must be ensured with appropriate technical solution to enable connection of the stored data - unless it is allowed by the law - directly and assigned to the concerned person.

8.5. During automated processing of the personal data the data controller and processor will ensure with further measures:

a.) prevention of unauthorized data entry;

(b) prevention of the use of automatic data-processing systems by unauthorised persons by means of data transmission equipment;

(c) the controllability and verifiability to which bodies have been or may be transmitted the personal data using the data transmission equipment;

d.) the controllability and verifiability when and by whom were the personal data entered into the automatic data processing systems;

e.) the recoverability of installed systems in the event of a malfunction and

f.) to report errors in automated processing.

8.6. The controller and the processor shall take into account the current technological development when defining and applying measures to ensure the security of the data. Among several possible processing solutions, one should choose which ensures a higher level of protection of personal data, unless this would create disproportionate difficulties for the controller.

9. Rights of concerned persons

9.1. The concerned person may request the Service Provider to provide information about the processing of his/her personal data, may request rectification of his/her personal data or required the erasure or blocking of his/her personal data, with the exception of compulsory data processing.

9.2. At the request of the concerned person the data controller gives information about the following - the data managed, the data processed by him or the data processor appointed by him, about their sources, the purpose, the legal basis, the duration of the data management, about the name, the address of the possibly involved

data processor, as well as - in case of transferring the personal data of the concerned - about the legal basis and the addressee of the data transfer.

9.3. For the purpose of controlling legal conditions of data transfer and information of the concerned person the data controller keeps a record, which includes the date of the transfer of personal data managed by him/her, the legal basis and addressee of data transfer, the determination of the sphere of transferred personal data, and the other data specified by the rule describing data management.

9.4. The data controller is obliged to give the information for the relevant request of the concerned person in writing within maximum 30 days reckoned from submission of the request, without any compensation and condition.

9.5. At the request of the user the data controller gives information about the data managed by him/her their sources, the purpose of data management, the legal basis and duration thereof, possibly about the name, address and data management-related activity of the data controller, as well as - in case of transferring the personal data of the concerned person, - about the legal basis and addressee of data transfer. The data controller is obliged to give the information for the relevant request of the concerned person in writing within maximum 30 days reckoned from submission of the request, without any compensation and condition.

9.6. The services provider shall correct the personal data, if it does not comply with reality and the appropriate correct personal data is available.

9.7. Instead of deletion, the Service Provider locks the personal data if the User so requests, or if, based on the information available to him/her, it can be assumed that the deletion would harm the legitimate interests of the User. The blocked personal data shall only be managed as long as the data processing purpose which excluded the deletion of the personal data exists.

9.8. The Service Provider deletes the personal data if management is unlawful, the User requests, the processed data is incomplete or erroneous - and this condition is not legally remediable - provided that the deletion is not excluded by law, the purpose of data processing is terminated or the data storage deadline established by law has expired, it has been ordered by the court or the National Authority for Data Protection and Freedom of Information.

9.9. The controller shall mark the personal data processed by him/her if the data subject disputes its correctness or accuracy, but the inaccuracy or inexactness of the contested personal data cannot be clearly established.

9.10. Rectification, blocking, marking and deletion shall be notified to the data subject and to all persons to whom the data were previously transmitted for the purposes of data processing. Notification may be omitted if this does not prejudice the legitimate interest of the data subject with regard to the purpose of the processing.

9.11. If the controller fails to comply with the data subject's request for rectification, blocking or deletion, he/she shall provide in writing the factual and legal reasons for refusing the request for rectification, blocking or deletion within 30 days of receipt of the request. In the event of refusal of a request for rectification, deletion or blocking,

the controller shall inform the data subject of the possibility of remedy and of appealing to the Authority.

10. Data Protection Incident

10.1. The data protection incident shall be notified by the controller to the competent supervisory authority without undue delay and, if possible, no later than 72 hours after the personal data breach becomes aware, unless the personal data breach is unlikely to be at risk of the rights and freedom of natural persons. If the notification is not made within 72 hours, it shall be accompanied by reasons justifying the delay.

The notification to the supervisory authority shall at least:

- describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects and the approximate number of categories of data subject to the incident;
- the name and contact details of the data protection officer or other contact point providing further information shall be provided;
- the likely consequences of the personal data breach shall be described;
- the measures taken or planned by the controller to remedy the personal data breach, including, where appropriate measures to mitigate any adverse consequences resulting from the personal data breach must be specified.

10.2. The Processor shall notify the data breach to the controller without undue delay after becoming aware of it.

10.3. If and where it is not possible to communicate the information at the same time, it may be provided in instalments without further undue delay.

10.4. The Data Controller records data breaches, indicating the facts relating to the personal data breach, its effects and the measures taken to remedy it. Such records shall enable the supervisory authority to verify compliance with the handling of personal data breaches.

10.5. Where the personal data breach is likely to entail 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.

The information provided to the data subject shall clearly and comprehensively describe the nature of the personal data breach and at least provide the information and measures specified in Section 11.1 of this Policy.

10.6. The data subject need not be informed in accordance with point 11.5 if any of the following conditions is met:

- the controller has implemented appropriate technical and organisational protection measures and those measures have been applied to the data affected by the personal data breach, in particular those measures, such as the use of encryption, which are intended to make the data unintelligible to persons who are not authorised to access it;

- the controller has taken further measures following the data protection incident to ensure that the high risk to the rights and freedom of the data subject referred to in point 11.1 are no longer likely to be realized;
- the information would require a disproportionate effort. In such cases, data subjects shall be informed by means of publicly disclosed information or similar measures shall be taken to ensure that data subjects are equally effectively informed.

11. Legal remedy

11.1. The person concerned may object to the processing of his/her personal data if

a) the processing or transfer of personal data took place without the consent of the data subject, unless the processing is ordered by law;

(b) the use or transfer of personal data is for the purposes of public opinion polling or scientific research;

c) in other cases as defined by law.

11.2. The Data Controller shall examine the objection within the shortest possible time and within a maximum of 15 days from the submission of the application, make a decision on its merits and inform the applicant in writing of its decision. If the Service Provider establishes the validity of the data subject's objection, the data processing, including further data recording and data transmission, shall cease, the data will be blocked, and all those shall be notified to whom the personal data subject to objection have been transferred earlier and who are obliged to take action to enforce the right to object.

11.3. If the data subject disagrees with the decision of the controller, the data subject may, within 30 days of its communication, go to court. The court is acting out of turn.

11.4. Complaints against a possible infringement by the data controller may be lodged with the National Authority for Data Protection and Freedom of Information:

National Data Protection and Freedom of Information Authority
1125 Budapest, Szilágyi Erzsébet avenue 22 / C.
Correspondence address: 1530 Budapest, P. O. box: 5.
Phone: +36 -1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu

Budapest, 1st April, 2018