PRIVACY POLICY

Effective from 25 of May, 2018

*The manager of PROOFIT Informatics LLC. ("**Company**") orders the implementation of the following policy, in order to*

adhere to Regulation 2016/679 ("GDPR") of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, effective from 25 of May, 2018;

comply with Act CXII. Of 2011 on Informational Self-Determination and Freedom of Information in cases outside the scope of the GDPR

ensure the protection and the lawful, fair and transparent management and processing of the personal data of natural person clients, employees and any other people in relation with ProofIT Informatics Kft.

I. Details of the data controller

Company name of the data controller: ProofIT Informatikai Kft.
Address of the data controller: 1112 Budapest, Törökbálinti way 24/A
Company registration number of the data controller: 01-09-879856
Tax identification number of the data controller: 13919207-2-43
Phone number of the data controller: [+36 1 203-2250]
Electronic contact of the data controller: [info@proofit.hu]

II. Definition of concepts

Within the scope of this Policy:

1. **"data controlling"**: Any operation executed automatically or not automatically on the personal data or data sets, that the Company carries out within its regular business activity, including but not limited to collection, capture, systematization, storage, utilization, transfer, synchronization or linking, restriction, deletion and destruction.
2. **"data controller**": It is the Company from the definition of article 4 (7) of the GDPR
3. **"personal data breach":** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed
4. **"Authority"**: Hungarian National Authority for Data Protection and Freedom of Information
5. **"personal data"**: means any information 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, an identification 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.
6. **"client"**: Natural person with an established contractual obligation with the Company for an activity that is within its regular business activity.
7. **"data processor":** the natural or legal person, public authority, agency or any other body that processes personal data in the name of the data controller.

8. **“recipient”:** natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
9. **“the data subject’s consent”:** Any freely and expressly given specific and informed indication of the will – in the form of a statement or unambiguous action of agreement- of the data subject by which he signifies his agreement to personal data relating to him being processed fully or to the extent of specific operations.

III. Duration and purpose of the policy

10. The purpose of this Policy is to ensure that each executive officer and employee of the Company, or any other person in an employment type legal relationship with the Company complies with the legal regulations of data protection in effect during their activities. The executive officers and employees of the Company, or any other person in an employment type legal relationship with the Company shall adhere to the provisions of the GDPR, the Information Law and this Policy when controlling the personal data of the natural person clients in relationship with the company or of any other natural person.
11. The company shall abide by the following principles determined in the laws of data protection when processing personal data:
    a. *legality, fair dealing and transparency:* the data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
    b. *purpose limitation:* collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
    c. *data minimization:* adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
    d. *accuracy:* accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
    e. *storage limitation:* kept 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject
    f. *integrity and confidentiality:* processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures

g. *accountability:* The controller shall be responsible for, and be able to demonstrate compliance with all of the above

12. The Company shall proceed with its data protection activities in a manner that complies with the principles of data processing and which abides by the legal requirements of data protection in effect with the purpose of accountability and the protection of the rights and freedom of the owner of personal data.

IV. Data controlling by the Company:

13. All data controlling activities of the company belong under the terms of data protection. The company is only entitled of personal data related data controlling, if it possesses a title for it.
14. Processing shall be lawful only if and to the extent that at least one of the following applies:
    a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
    b. processing is necessary for compliance with a legal obligation to which the controller is subject;
    c. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    d. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.
15. The Company can use the services of a data processor for its data protection activities.

IV/A. Client related data controlling

16. The purpose of data controlling according to this subchapter is:
    a. the creation or maintenance of contractual obligations between the Company and the data subject that stem from the regular business activity of the Company (e.g.: agency agreement, sales contract) or the exercise of legal rights in relation with these contractual obligations (e.g.: claim of consideration) and the discharge of duties (e.g.: fulfillment of obligations agreed in a contract)
    b. the assertion and protection of legal rights of the Company in relation to the clients
    c. the discharge of legal duties which might fall on the Company from any contractual obligation.
17. Legal grounds for data control:
    a. The data subject has consented to the processing of their data
    b. Paragraph 13/A (3) of Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services: “the service provider may – for the purpose of providing the service – process personal data indispensable for providing the service for technical reasons. Should other conditions be identical, the service provider shall select and operate the means applied in the course of providing information society service at all times, so that personal data be processed only if it is absolutely indispensable for providing the service or

achieving other objectives stipulated in this Act, and only to the required extent and duration."

18. Duration of data controlling according to this subchapter: From the personal data subject's consent to 5 years after the end of the contractual obligations. For all personal data processed based on consent that belongs under the term of Act LIII. of 2017, §56-57. about the prevention of money laundering and terrorism, the duration of data controlling lasts 8 years after the end of contractual obligations.
19. Method of data control according to this subchapter: management of paper-based or electronic databases or execution of electronic or paper-based operations on personal data.
20. People entitled to access personal data or recipients of personal data: all personal data shall be accessed and processed only by the sales and marketing personnel of the Company in compliance with the provisions of this Policy.
21. Any type of data control mentioned in this subchapter is only lawful to the extent the company possesses the sufficient title. In case this title stems from consent-based data control (paragraph 14. a.), then the criterion for lawfulness is that the Company proceeds with its activities in compliance with the provisions of this subchapter.
22. The Company is authorized -within the boundaries of consent-based data control- to access and manage the following data of the client:
    a. personal identification information of the natural person
    b. depending of the nature of the contractual legal relationship, the data subject's bank account number and the name of the financial institution where this bank account is opened, if it is included in the contract
    c. contact information of the data subject (phone number, email address)
    d. in case of a legal person partner, the following information of the natural person holding the power of representation of the legal person: first and last name, office, place and date of birth, mother's maiden name, permanent address or for the lack of thereof, residential address.
23. During the consent-based data control, the Company is obliged to inform the data subject (client), before the establishment of any contractual obligation and simultaneously with reaching out to the client, of the following:
    a. name and contact information of the Company and the representative of the Company
    b. of the fact, that any contractual obligation can only be established if the data subject gives their consent to the Company to access and manage any personal data that is needed, and also of the possibility to withdraw consent
    c. the specific purpose, legal grounds and extent of data control
    d. the recipients and categories of personal data
    e. the expected duration of the storage of personal data
    f. the data subject's rights
    g. the possibilities of lodging a complaint to the Authority or requesting legal remedy.

    The Company shall provide this information by forwarding and making Appendix 1. available to the data subject.
24. The Company shall provide this information to the data subject in brief and plain language. In addition to this, the Company is required to make this Policy available to the client and forward it in an electronic form to the clients contact information if requested.
25. Following the reception of information, the data subject is entitled to freely decide, whether they wish to establish contractual obligations with the Company. The consent of the client is considered lawful, if the following conditions are met:

a. it is voluntary;
b. it is with regards to a specific data control process (concerning one or more given contractual obligations);
c. it is based on adequate informing;
d. it is an unambiguous indication of will.

26. The condition for data controlling based on the consent of the data subject, is that previous to establishing a legal relationship with the Company, the data subject has acknowledged and agreed to the Company's Privacy Policy, the purpose of the Company's data controlling activities, the concept of data controlling and the type of data to be accessed and processed, and expressed their consent by signing the agreement, the contents of which are identical to Appendix 2.
27. In case of contractual relationships, the Company is entitled to create the consent statement of the client as the data subject within the provisions of the contract to be signed by the Company and the client. By signing a contract containing a consent statement, the client consents to their personal data to be accessed and processed by the Company.
28. In their consent statement the client shall state, in addition to the consent-based data control, that they have explicitly understood the information provided by the Company regarding the fact that the Company may be entitled to the processing of the client's data based on other titles as well.
29. If the data subject does not consent to the processing of their personal data or refuses to sign the agreement the contents of which are identical to Appendix 2., then the Company cannot establish contractual obligations with the given natural person. The data subject can withdraw their consent anytime. Withdrawing the consent does not influence the lawfulness of the consent-based data processing previous to the withdrawal.
30. The Company is obligated to delete from its databases all personal data, that belongs to subjects with whom the contractual obligations were for any reason terminated, except for cases where the data subject has consented to the further processing of their personal data or where the keeping of data is required by the law (e.g.: in case of legal relationships involving tax law)

IV./B. Data controlling in case of the hiring process

31. During the hiring process the Company is entitled to access the personal information of the natural person that has applied to the position offered by the Company, which they provided in their application and directly or indirectly delivered to the Company. The applicant shall consent to this through a statement, that is identical to the contents of Appendix 4 of this Policy. The consent of the applicant is considered lawful only if the following conditions are met:
    a. it is voluntary;
    b. it concerns the evaluation of the application;
    c. it is based on adequate informing;
    d. it is an unambiguous indication of will.

    The Company considers the applicant's consent statement lawful in every case. The possible illegality of the consent statement has to be proven by the subject.
32. In any advertisement with the intent of hiring, the Company is obligated to indicate, that by applying the applicant agrees to their personal data given in their application to be processed by the Company, and by submitting their application they explicitly consent to their personal data being accessed and processed by the Company. After receiving the application, the Company is required to inform the applicant of the data control regarding

their personal data (through the information procedure part of Appendix 3) and -in case they have not given their consent- inform them about the ways they can give their consent. Before the applicant gives their consent, the Company is not entitled to access any of their personal data given in their application. In the email the Company sends to establish contact, it is mandatory to bring the applicant's attention to the fact that the Company completes data processing activities regarding the personal data included in their application, and by responding to the email (with an application-type content) or by a confirmation that they have read the email they explicitly give their consent to the company to access and process these personal information.

33. The Company can only access and process the personal data given in the application for hiring purposes, to decide the aptness of the candidate. If the hiring process of the given candidate is unsuccessful or the Company's offer has been rejected by the applicant, then the Company shall delete all personal data (except for consent statement and the information included in it) of the applicant without delay, and inform the applicant about this. In this case, the consent statement is preserved for the normal limitation period, for protecting and pursuing legitimate interests. If the hiring process results in success, then the personal data given by the applicant, that the company is entitled to process, form part of the personal data of the employee, to the processing of which the employee to be is required to consent before signing the contract of employment.
34. The Company cannot gather any other personal information about the applicant apart from those that were provided in the application, and cannot use it during the evaluation process as a filter, except for pursuing the legitimate interest of the Company, if during the examination of the applicant's social media profile encounters information, that is not included in the application, but is relevant for fulfilling the given position.

IV./C Data control of the executive officers and employees of the Company, or of any other person in an employment type legal relationship with the Company

35. The Company is entitled to handle the personal data of the executive officers and employees of the Company, or of any other person in an employment type legal relationship with the Company, if the following conditions are met:
    a. the data subject has consented to the data control (e.g.: consent for the further use of the data given for the hiring process, bank account number for transferring the salary, copy of the proof of qualifications);
    b. it is needed for fulfilling a contract (e.g.: managing records);
    c. it is needed for fulfilling legal obligations (e.g.: fulfilling tax obligations);
    d. it is needed for pursuing legitimate interests of the Company (or the employee).
36. Purpose of data control according to this sub-chapter: establishment and maintenance of legal relationship concerning the performance of executive officer tasks, employment, or any other employment-type legal relationship with the Company, and the exercise of any legal right derived from these and the discharge of duties (e.g.: tax advance payments), or the termination of legal relationship.
37. Duration of data control according to this subchapter:
    a. in case of data control as a legal obligation, the duration is determined by the relevant law
    b. in case of a consent statement given by the data subject, the beginning of the data control period is the signing of the agreement containing the consent and it ends 5 years after the termination of the legal relationship
    c. For all personal data processed based on consent that belongs under the term of the Act LIII. of 2017, § 56-57. about the prevention of money laundering and

terrorism, the duration of data controlling lasts 8 years after the end of contractual obligations.

38. Method of data control according to this subchapter: management of paper-based or electronic databases or execution of electronic or paper-based operations on personal data. By giving a consent statement, the data subject explicitly agrees that the Company has the right to make a copy or an electronic copy of the documents containing personal information or of any other document that is needed for the establishment and maintenance of executive officer legal relationship, employment, or any other employment-type legal relationship with the Company, and to preserve these documents through these copies. The Company is required to store these copies together with all other documents of the subjects in a place, where no unauthorized person can access them.
39. Types of personal data involved in data control according to this subchapter:
    a. the subject's first and last name, maiden name (if applies), place and date of birth, mother's maiden name, permanent address or for the lack of thereof, residential address, personal identification number, identity card number, tax identification number, and any other information that the Company is required to access (without the subject's consent, to fulfill its legal obligations), including but not limited to the personal data contained in personal records of executive officers and employees, working hours register, register of vacation days, salaries, travel expenses, labor safety training, and medical fitness.
    b. The subject's bank account number, and the name of the financial institution where this bank account is opened, in case the data subject gets their salary by bank transfer and provided explicit consent for accessing the copy of the proof of qualifications and the relevant personal data.
    c. data that is needed for the fulfillment of the contract or for pursuing the legal interests of the Company (or the employee) (e.g.: protection of property, liability)
40. Natural persons in an executive officer legal relationship, employment, or any other employment-type legal relationship with the Company, in order to establish, maintain or terminate this legal relationship, are required to consent to data control by signing the agreement in Appendix 6. of this Policy previous to establishing the legal relationship.
    Before signing the agreement in Appendix 6., the Company shall inform the data subject of the following:
    a. name and contact information of the Company and the representative of the Company;
    b. of the fact, that any executive officer legal relationship, employment, or any other employment-type legal relationship with the Company can only be established if the data subject gives their consent to the Company to access and manage any personal data that is needed;
    c. the specific purpose, legal grounds and extent of data control;
    d. the recipients and categories of personal data;
    e. the expected duration of the storage of personal data;
    f. the data subject's rights;
    g. the possibilities of lodging a complaint to the Authority or requesting legal remedy.

    The Company shall provide this information by using Appendix 5.
41. The ompany shall provide this information to the data subject in a brief and plain language. In addition to this, the Company is required to make this Policy available to the natural person in an executive officer legal relationship, employment, or any other

employment-type legal relationship with the Company, and forward it in an electronic form to their contact information if requested.

42. Following the reception of information, the data subject is entitled to freely decide, whether they wish to establish executive officer legal relationship, employment, or any other employment-type legal relationship with the Company. The consent of the data subject is considered lawful, if the following conditions are met:
    a. it is voluntary;
    b. it is with regards to establishing, maintaining or terminating executive officer legal relationship, employment, or any other employment-type legal relationship, and with regards to exercising any rights and discharging any duties that stem from this legal relationship;
    c. it is based on adequate informing; and
    d. it is an unambiguous indication of will.
43. The Company is obligated to delete from its databases all personal data, that belongs to subjects with whom the executive officer legal relationship, employment, or any other employment-type legal relationship was for any reason terminated, except for cases where the data subject has consented to the further processing of their personal data, where the keeping of data is required by the law (e.g.: in case of legal relationships involving tax law) or it is required for pursuing the legal interests of the Company. In case the contract of the executive officer, employee or of any other person in an employment-type legal relationship with the Company included a non-compete clause, then the Company is allowed to follow the social media platforms of the data subject for a period of time determined by the non-compete clause after the termination of the legal relationship, in order to monitor if the subject complies with the agreements of the non-compete clause. If the subject does not act in accordance with this agreement, the Company is entitled to use the relevant data to pursue its legal interests. The subject consents to this use of their data by acknowledging this Policy and by giving their consenting statement defined in point 38.
44. Apart from the previously defined data, the Company is not entitled to monitor the social media platforms of the executive officers, employees or of any other person in an employment-type legal relationship with the Company, nor gather personal data from these sites. The Company cannot make mandatory the use of personal social media platforms, that are in the exclusive management of the subject, to serve the interests of the Company (e.g.: expanding the client base through acquaintances).
45. To comply with Act V. of 2013 on the Civil Code, Act I. of 2012 on the Labor Code, the Company's interests and with the maintenance of the Company's regular business activity, the executive officers, employees or of any other person in an employment-type legal relationship with the Company can only carry out activities on the Company's assets that are within the boundaries of their job responsibility and are connected to the regular business activity of the Company. Regarding this, these people shall acknowledge, that the logging done by the assets, and therefore also the data control of the Company, is lawful even in cases where the data logged forms part of the private or family-life of the executive officer, employee or of any other person in an employment-type legal relationship. The subjects explicitly consent to this with their statement in paragraph 38. To prevent having to control personal data that is part of the subject's private or family life, despite the prohibition, the Company is entitled to restrict the access of certain websites and services. This restriction shall be done in the appropriate time and with the presence of the subjects. Within the restriction of the use of assets for private purposes, the Company might order for example the blocking of access to social media sites.

46. During home office and remote work, the Company is entitled to access the data related to the device, the data logged by the private device that is being used for work purposes, and concerns the executive officer, employee or of any other person in an employment-type legal relationship with the Company, with the condition, that it abides by the principle of proportionality and thus does not access any private data stored on the device and its data control does not involve the private and family life of the data subject.
47. In the information provided to the executive officers, employees or of any other person in an employment-type legal relationship with the Company, the Company is required to draw the attention of the subjects to the fact, that if the Company possesses, and makes available for use a device, that monitors its location (even outside of working hours), then the Company is only entitled to access the location data to check the device's location for property security reasons. This data control outside of working hours cannot be used for accessing the (supposed) location of an executive officer, employee or of any other person in an employment-type legal relationship with the Company. If the given device's properties allow it, the Company shall provide the possibility of turning off the location services of the Device when using it for private purposes outside of working hours.

IV/F. Data control regarding online visitors

48. By using the www.proofit.hu website and by subscribing to the newsletter (not in operation at the effective date of this Policy) through the website, the company is entitled to control certain personal data of the people that visit the website ("Users"), based on their voluntary consent to data control for pre-determined and specified purposes (providing newsletters and storing user data to improve user experience).
49. The Company is only entitled to use the User's personal data given on the website for newsletter services for business purposes, if the User has previously provided consent. In case the user consents to their personal data to be used for business purposes, then this type of data control is valid until the withdrawal of consent or until 2 years after opening the last newsletter.
50. The User shall indicate their demand for newsletter services by activating the website's command titled "Subscribe", and by giving access to the necessary personal information. The personal data needed for providing newsletters include the following:
    a. Users first and last name
    b. electronic mailing address (email) managed by the User
    c. date of the subscription and IP address at the time of the subscription (to execute technical operations)
51. The purpose of data control is to deliver electronic messages to the User, containing relevant professional content, white papers and advertisements to provide information of the latest products, offers, functions, etc.
52. Legal grounds of the data control:
    a. The explicit consent of the data subject to use their personal data for marketing purposes;
    b. Paragraph 6 (5) of Act XLVIII. of 2008 on Essential Conditions of and Certain Limitations to Business Advertising Activity: "Advertisers, advertising service providers and publishers of advertisement shall maintain records on the personal data of persons who provided the statement of consent to the extent specified in the statement. The data contained in the aforesaid records, relating to the target of the advertisement, may be processed only for the purpose defined in the statement of consent, until withdrawn, and may be disclosed to third persons subject to the express prior consent of the person affected".

53. The consent of the user is only considered lawful, if the following conditions are met:
    a. it is voluntary;
    b. it concerns the use of the newsletter service;
    c. it is based on adequate informing;
    d. it is an unambiguous indication of will.
54. Previous to indicating their demand for newsletter services, the Company shall inform the User of the process of User related data control, defined in this subchapter. The User shall acknowledge that they have received this information by giving their consent electronically, that contains the agreement with the data control based on this subchapter. Giving this consent is indicated by checking the box on the electronic interface, which is also the prerequisite of sending their request for newsletter to the Company.
55. The lack of consent of the User to data control for newsletter services can result in the Company failing to deliver newsletters or any other direct marketing message.
56. People entitled to access personal data or recipients of personal data: all personal data shall be accessed and processed only by the sales and marketing personnel of the Company in compliance with the provisions of this Policy.
57. The Company reserves the right to suspend the newsletter service for a given User, if it is brought to their attention, that the User utilizes the newsletter for purposes outside of normal use, especially if this involves damaging the good reputation of the Company related to its regular business activities.
58. The Company shall not send any unsolicited marketing messages and the User has the right to unsubscribe freely and without any limitation from receiving offers. In this case the Company shall delete all marketing related data of the User, and shall cease to send additional messages. The User shall unsubscribe by clicking on the link included in the emails.
59. The withdrawal of the consent is effective without regard to the acknowledgment of the Company, and following the withdrawal the Company is no longer entitled to provide newsletter services to the given User.
60. The www.proofit.hu website, managed by the Provider, can store and control data in the end-device of the User with the help of cookies based on the act of the User visiting the website, with the purpose of identifying and tracing the User, facilitating their further visits, delivering tailored content and advertisements and conducting market research. The User has to agree to the use of cookies in all cases, by activating the “Accept” icon on the website next to informational text “This website uses cookies to provide you with the best browsing experience. Find out more or adjust your settings”.
61. The User does not have to accept the use of cookies to visit the website, however, the lack of consent can lead to the sub-optimal functioning of certain pages of the website, and the website can deny access to certain information. By activating the “settings” icon next to the “Accept” icon, the website will redirect the User to the website’s Privacy Policy and cookie settings.
62. The Company obtains automatically certain data of the User through the website. These include the following:
    a. Information of the device providing connection to the website through an open network;
    b. IP address used by the User;
    c. dates and times.

    The sole purpose of the control of these data is to obtain website traffic data and to detect and log any website related problems and attempts at attacking the website. The legal ground for this data control is based on the User’s consent and the protection of the legal interests of the Company. The Company fulfills the requirement of informing by

publishing the contents of this subchapter on their website, and the User expresses their acknowledgement and agreement by visiting the website, understood as implied conduct.

63. The User is exclusively responsible for not letting their username and password used on the Company's website to be accessed by unauthorized third parties and for not losing or destroying it nor telling it to third parties. The Company cannot be held liable, if the User manages their username, password or any other data given on the website differently from this Policy or the provisions of the laws in effect, makes them accessible for unauthorized third parties, tells these parties, loses or destroys them, and as a consequence faces the risk of legal disadvantage.
64. The duration of data control according to this subchapter: 2 years from the Company recording the personal data.

Cookie type	Legal ground for data control	Duration of data control	Processed data
Work session cookies	Paragraph 13/A §(3) of Act CVIII. of 2001 about certain issues of electronic commerce services and information society services	The period lasting until the termination of the relevant visitor session.	connect.sid

V. Data processors

65. The Company utilizes the services of a hosting service provider, that provides reseller hosting services.
    a. The Data processor is entitled to access all personal data given by the Users that access the proofit.hu website, for the purpose of making the website accessible and fully operating.
    b. Duration of data processing: the data processing lasts until the termination of the agreement between the Company and the Data processor or until the data subject submits a request to the data processor for deletion.
    c. Legal ground for data processing: The explicit consent of the data subject and paragraph 13/A (3) of Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services.
    d. Name and address of the data processor: Webber Digital Solutions Kft., 1085 Budapest József boulevard 69., phone: +36 30 525 0954, email: hello@webber360.com, website: webber360.com
66. The Company also utilizes the data processing services of a newsletter services provider, that provides online newsletter sending services.
    a. Name and address of the data processor: MailChimp c/o The Rocket Science Group, LLC, 675 Ponce De Leon Ave NE, Suite 5000 Atlanta, GA 30308 USA Website: https://mailchimp.com

VI. Social media sites

67. The Company accesses the name and profile picture of all person who has registered on the social media sites of Facebook/Google+/Twitter/Pinterest/YouTube/Instagram and has liked the webpages, for the purpose of sharing, liking and promoting the website, its contents or products, services, offers.
68. The data controlling is done on the social media sites; therefore the data protection policies of these sites apply for the duration and method of the data control, and for the possibilities of deletion and modification of personal data.
69. The legal grounds for this data controlling in the voluntary consent of the subject to their personal data to be processed on the social media sites.

VII. Utilization of Google AdWords and Google Analytics

70. The Company utilizes the “Google AdWords” online advertising program and within that uses Google’s conversion tracking services. The conversion tracking is an analytical service of Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; „Google “).
    a. When the User accesses the website through an ad by Google, then their computer receives a cookie for conversion tracking. These cookies have only limited validity, and do not contain any personal data, thus the User cannot be identified through them.
    b. If the cookie has not yet expired and the User is browsing certain pages of the website, then both Google and the Company can see that the User has clicked on the advertisement.
    c. Each Google AdWords User receives a different cookie, therefore these cannot be tracked through the websites of AdWords’ clients.
    d. The information obtained by Google and the Company with the help of conversion tracking cookies serves the purpose of creating conversion statistics for the clients of Google AdWords. Thus, the clients can be informed about the number of users that have clicked on the advertisement and have been forwarded to the website equipped with a conversion tracking tag. However, no personal data is accessed by which the users could be identified.
    e. In case the User does not wish to partake in conversion tracking, they can decline this by blocking the installation of cookies in their browser. Subsequently the User will not be part of the statistics of conversion tracking.
    f. More information and Google’ Privacy Policy can be accessed by the following link: https://www.google.de/policies/privacy/
71. The Company utilizes the services of the Google Analytics application, which is the web analytics service of Google Inc. Google Analytics utilizes text files, “cookies”, that are installed on the Users computer and facilitate the analysis of the website visited by the User.
    a. The information related to the website visited by the User and generated by cookies is stored on one of Google’s servers in the USA. By activating the website’s IP-anonymization, Google shortens the User’s IP address within the member states of the European Union or in other states that form part of the European Economic Area.

b. Only in exceptional cases can the full IP address delivered to Google's USA-based servers and shortened there. Based on the commission of the website's operator, Google uses the information gathered to analyze how the website was used and to create reports of the activity on the website and to provide other services in relation with the use of the website.
c. Within the frameworks of Google Analytics, the IP address provided by the User's browser will not be connected to Google's other data. The User can restrict the use of cookies by changing the settings of their browser, however, as a consequence some functions of the website might not be available. Moreover, the User has the right to prevent Google from collecting and storing data collected by cookies about the website usage of the User by downloading and installing the following browser plugin:
https://tools.google.com/dlpage/gaoptout?hl=hu

VIII. The data subjects' rights

72. The natural persons, whose data are by any reason controlled by the Company, are entitled to the following rights:
    a. right to information and access to personal data;
    b. right to rectification;
    c. right to erasure;
    d. right to restriction of processing;
    e. right to data portability;
    f. right to object.
73. The data subject can exercise their rights defined in this chapter by submitting their application to the Company. The data subject can propose their application electronically, on paper through universal postal service or on paper through handing it over to the representative executive officer, employee or any other person in an employment-type legal relationship with the Company at the Company's Offices.
74. The person who is entitled to manage applications shall forward them the without delay to the management. The Company's management shall examine the application immediately after receiving it. If they find that it is obviously ill-founded or was put forward by an unauthorized person, all further examination will be denied. If it is not obviously ill-founded and was put forward by an authorized person, then the application will be substantially examined. The management will notify the application's proposer about their decision (rejection or acceptance) and the completed or proposed steps within 30 days from receiving the application.

VIII/A Right to rectification

75. The data subject shall have the right to obtain from the Company without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
76. The data subject (or their authorized representative) shall put forward their application for rectification by filling out Appendix 8 or issuing a statement with identical contents and delivering it to the Company. If the personal data is contained in a public document (e.g.: documents prepared by administrative agencies), then the applicant shall present it, and

hand over a copy to the Company of the public document verifying the contents of the personal data.

VIII/B Right to erasure

77. The data subject shall have the right to obtain from the Company the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
    a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
    b. the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
    c. the personal data have been unlawfully processed;
    d. the personal data have to be erased for compliance with a legal obligation to a law to which the Company is subject.
78. The data subject shall put forward their application for erasure by properly filling out Appendix 9 or issuing a statement with identical contents and delivering it to the Company.
79. The Company can refuse the erasure of personal data, if any of the conditions of article 17 (3) of the GDPR are met.

VIII/C. Right to restriction of processing

80. The data subject shall have the right to obtain from the Company restriction of processing where one of the following applies:
    a. the accuracy of the personal data is contested by the data subject, for a period enabling the Company to verify the accuracy of the personal data;
    b. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
    c. the Company no longer needs the personal data for the purposes of the processing, but they are required to further (restricted) data control by the data subject for the establishment, exercise or defense of legal claims;
    d. the data subject has objected to processing, for the duration while the verification is pending whether the legitimate grounds of the controller override those of the data subject.
81. The data subject (or their authorized representative) shall put forward their application for rectification by filling out Appendix 10 or issuing a statement with identical contents and delivering it to the Company.
82. Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims of the data subject, or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or of a Member State.
83. In case the conditions of data restriction are not met, the data subject shall be informed by the controller before the restriction of processing is lifted.

VIII/D. Right to data portability

84. The data subject shall have the right to receive the personal data concerning him or her, that the Company processes in an automated way based on the consent of the data subject, in an electronic format, according to article 20 (1) of the GDPR.
85. When providing their data to the data subject, the Company shall keep in mind that the data subject is entitled to transmitting the gathered and stored data to a different controller, and the data subject shall have the right to request the Company to have the personal data transmitted directly from one controller to another, where technically feasible.
86. The data subject (or their authorized representative) shall put forward their application for rectification by filling out Appendix 11 or issuing a statement with identical contents and delivering it to the Company.

VIII/E. Right to object

87. The data subject shall have the right to object at any time to processing of personal data concerning him or her by the Company, in case the data control is done for pursuing the legal interests of the Company or a third party.
88. The data subject (or their authorized representative) shall put forward their application for rectification by filling out Appendix 11 or issuing a statement with identical contents and delivering it to the Company.
89. Following the acceptance of the statement of objection, the Company shall no longer process the personal data to pursue the legitimate interests of the Company or of a third party, unless the Company 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.
90. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
91. Automated decision making in unique cases, including profiling: 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.
92. The previous paragraph does not apply in the following cases:
    a. the decision is required for establishing or fulfilling a contract between the data subject and the company;
    b. the decision is made possible by the law of the European Union or of a Member State concerning the data controller, that also includes provisions for the protection of the data subject's rights, freedom and legal interests;
    c. the decision is based on the explicit consent of the data subject.

93. The Company shall inform the data subject of the measures taken following the aforementioned applications without delay, but no later than 30 days from receiving the application.
94. If necessary, this period can be extended with an additional 60 days. The Company shall inform the Data subject about the extension of the deadline together with the reasons for the delay, within 30 days from receiving the application.

95. If the Company does not take any measures following the subject's application, then it shall inform the data subject about the reasons for this and of the possibility to file a complaint to the Authority or seek legal remedy without delay, but no later than 30 days from receiving the application.

IX. Data Protection Officer

96. The data controlling activities of the Company – in accordance with the workgroup guidelines of article 29.- does not require the appointment of a Data Protection Officer from articles 37-39. of the GDPR.

X. Data security and the process of data storage

97. The Company executes the data control in manner, that complies with not just the provisions of the GDPR and other data protection laws, but also with the protection of the data subject's right to family and private life, and other rights and freedoms.
98. The provisions determined in this Policy regarding the storage of personal data refer to all data stored both in a paper-based way or electronically, that form part of the filing system or which the Company manages in a fully or partially automated manner. The Company shall use its own devices for electronic storage of the personal data, and stores the paper-based records in buildings under the ownership or use of the Company, which are used as seat, premise or branch.
99. The personal data collected and stored by the Company for data control shall only be processed solely for the purpose defined in this Policy on in the relevant laws, with the appropriate title.
100. The personal data collected and stored by the Company have to be kept during the data control period in a way that no unauthorized people can access it. The Company must ensure, that the collected and stored personal data:
    a. cannot be accessed or known by an unauthorized third person;
    b. shall not be subject to unauthorized data control;
    c. cannot be modified, forwarded, published or erased by an unauthorized person;
    d. shall not be forwarded in any different way from those mentioned in chapter VII.;
    e. shall not be modified, accidentally destroyed, deleted or made unavailable without authorization;
    f. shall be protected from loss and damage.
101. The Company shall consider the state and development of science and technology for their data control process and organizational activities. The Company shall apply the technology that guarantees the highest level of safety and is appropriate for the level of risk involved, in order to maintain data security and protect the rights and freedoms of natural persons.
102. The Company shall log its data control activities (Data Controlling Records) by using the template given in Appendix 13. and by adhering to the provisions of Article 30 of the GDPR. The Company shall do the administration of the Data Controlling Records

electronically and store it in paper format in a secure location, where no unauthorized person can access it.

XI. Transfers of personal data

103. The Company is not entitled to transfer or make accessible in any way any personal data under their processing or storage to external people, except for the following cases:
    a. The data transfer is required by law (e.g.: data collection for statistical purposes, or the employer's obligation to disclose data) and the recipient of the data -court, authority or other legal body- has delivered their official request to the Company.
    b. The data subject has given explicit consent to the transfer of their data, the recipient is in contractual obligations with the Company and the data transfer forms part of the fulfillment of the contractual obligation between the data subject and the Company.
104. The Company shall maintain records of the data transfer to ensure the lawfulness and to inform the subject, this record shall be based on the template given in Appendix 14 of this Policy, and shall include the date, the legal grounds and the recipient of the transfer, the description of the forwarded data, and other information determined by the laws relating to data control.
105. For the request defined in section 68, the Company shall provide the transfer of the stored personal data only to the extent needed to fulfill the request and only the requested quantity.
106. In case of data transfer related to section 68 of this policy, the Company is obliged to inform the Subject of the following:
    a. the name and address of the recipient or its representative;
    b. that they consent to the data transfer and acknowledge and related information;
    c. the specific purpose and extent of the transfer;
    d. the data subject's rights;
    e. the possibilities of filing a complaint to the Authority or requesting legal remedy.

    The data subject can give their consent to the specific data transfer at the same time with their consent of point 14. a., if at the time of the latter statement, the Company and the Subject are aware of the need for transfer. The data subject shall give their consent based on the template of Appendix 14.
107. In case of data transfer concerning the data of section 68, the Company is entitled to transfer only those data, that are indispensable for fulfilling the contractual obligations and to the transfer of which the data subject has given their explicit consent.

XII. Protocol to be followed in case of personal data breach

108. In accordance with article 4 (12) of the GDPR, a personal data breach is a breach of security, which can be:
    a. a breach of confidentiality, meaning the unauthorized disclosure of, or access to the personal data transmitted, stored or otherwise processed;
    b. a breach of access, meaning the accidental or unlawful destruction or loss of the personal data transmitted, stored or otherwise processed;

c. a breach of integrity, meaning the alteration of the personal data transmitted, stored or otherwise processed.

109. In case the Company's executive officer, employee or any other person in an employment-type legal relationship with the company suspects a breach of security in relation with the personal data collected and stored by the Company, they shall inform ("Signal") without delay the Company's management about their suspicion. Circumstances which cause a disruption in the data control systems and records that are contrary to the data protection policy of the company, are considered a breach of security. A breach of security does not necessarily mean that a personal data breach has occurred.
110. The Company's management shall examine and evaluate the situation without delay after having received the Signal. The investigation shall include each component of the circumstance that is suspected to have caused a breach of security, and the examination of each record and the state of all personal data.
111. The primary purpose of the management's investigation is to determine whether a security breach has actually occurred. If the investigation does not find any breach of security, then the proceeding shall be terminated, and the management shall document the investigation and log the results in accordance with Appendix 15 of this Policy.
112. If the management's investigation detects a breach of security, then the second step shall be to determine whether or not it also involved a personal data breach. In case there was no personal data breach, the management is required to take all the necessary steps to restore the security, then shall terminate the proceeding and shall document the investigation and log the results in accordance with Appendix 15 of this Policy.
113. If the results of the management's investigation show not only a security, but also a personal data breach, then the third step shall be to determine if the personal data breach involves a risk to the rights of the data subjects. In case the personal data breach does not involve this risk, the management is required to take all the necessary steps to restore the security, then shall terminate the proceeding and shall document the investigation and log the results in accordance with Appendix 15 of this Policy.
114. In case there was not only a security breach, but a personal data breach that results in a risk to the rights and freedoms of natural persons, the Company shall assess the extent of the risk. If the risk is significant, then the findings shall be documented and logged in accordance with Appendix 15 of this Policy. The Company shall notify the Authority or if needed, other data protection agency of the Member State.
115. If the management's investigation defined finds that the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay, apart from documenting and logging the results in accordance with Appendix 15 of this Policy and notifying the Authority or if needed, other data protection agency of the Member State.
116. The company as data controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, fulfil their obligations of notification. The Company is considered aware, if the Company's management can determine with confidence the occurrence of a security breach. After the assertion of this breach, the management shall evaluate the situation without delay.
117. In case the Company's management cannot finish its within the 72 hours set in section 122., they shall notify the authorities and inform the subjects and continue with the investigation. As soon as the findings of the investigation are available, the management shall provide supplementary notification/information or modifying notification/information.

118. The Company can fulfil their obligation for notification by filling out and delivering the electronic form provided by the Authority, or in case of a different data protection authority this can be done in the manner defined by the given authority. The notification shall include the following information:
    a. type of the personal data breach;
    b. the categories of the data subjects concerned;
    c. the approximate number of data subjects concerned;
    d. the categories of personal data records concerned;
    e. the approximate number of data records concerned.
119. The Company's management shall issue separate notifications for each personal data breach that involves a different data category.
120. The management is not required to issue a notification, if the personal data breach is not likely to have a high risk in relation to the rights and freedoms of natural persons. The Company's management shall assess the level of risk by taking into account all relevant circumstances of the case. Those circumstances that are not considered to result in any risk to the rights and freedoms of natural persons shall be proven and documented and the management shall take measures to restore safety.
121. The management shall fulfill their obligation to inform all concerned parties without undue delay by using the template given in Appendix 16. The management shall assess the nature of risk during the investigation by considering each circumstance of the case. Within these, the management shall take into account the following:
    a. the type of the personal data breach;
    b. the type of personal data affected by the breach;
    c. the sensitivity of the personal data affected;
    d. the extent to which personal data have been affected;
    e. the vulnerability of the natural person affected by the personal data breach.

    The risk concerning the rights and freedoms of natural persons is considered high if it can lead to the data subject suffering physical, material and non-material damages.
122. The Company's management shall inform the data subjects of the following:
    a. the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
    b. the name and contact details of the data protection officer or other contact point where more information can be obtained;
    c. the likely consequences of the personal data breach;
    d. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
123. The communication to the data subject shall be done in clear, plain and relevant language and without delay through a channel, by which the subjects are most likely to receive the information, based on the managers prediction. The Company can utilize more than one communication channels at the same time, in order to ensure the successful communication of the breach.
124. The communication to the data subject shall not be required if any of the following conditions are met:
    a. the personal data breach does not involve a high level of risk, as the Company has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

b. the Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize;
c. the risk resulting from the personal data breach is not considered high for any other reason.

125. Simultaneously with fulfilling the management's obligation to notify and inform, they shall also take any measure to eliminate the breach of security or of personal data after learning the results of the investigation. The Company shall -within its capabilities and as the circumstances permit- restore the integrity, accessibility and confidentiality of the affected personal data. The Company's management shall document the measures taken for the highest body of the Company by using the template given in Appendix 17.
126. If the Company fails to notify the data subjects about a personal data breach, then the Authority, after considering the level of risk being involved, can order the notification of the parties concerned.

XIII. Legal remedy

127. In case the data subject finds that the Company does not adhere to the provisions of data protection laws during its data controlling activities, for the protection of their rights they shall turn to the regional competent authority or to the Hungarian National Authority for Data Protection and Freedom of Information for a legal remedy.
128. Contact information of the Hungarian National Authority for Data Protection and Freedom of Information:
Address: 1125 Budapest, Szilágyi Erzsébet alley 22/C
Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
Email: ugyfelszolgalat@naih.hu
Website: http://naih.hu

XIV. Final provisions

129. **This Policy is effective from 25 of May 2018**. This Policy shall be applied to those legal relationships, that are established after this date, or to previously established legal relationships, that involve data controlling activities after 25 of May 2018.
130. **The Company shall inform all of its clients and all natural persons in legal relationship with the Company** about the effectiveness and the application of this Policy and shall make this Policy available for all concerned parties.
131. For the creation of this Policy, the following laws were taken into account:
a. Regulation 2016/679 of the European Parliament and Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
b. Act CXII. Of 2011 on Informational Self-Determination and Freedom of Information ("Privacy Act")
c. Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services (with special attention to § 13/A)

d. Act XLVIII of 2008 on Essential Conditions of and Certain Limitations to Business Advertising (with special attention to § 6)
e. Act XC of 2005 on the Freedom of Information by Electronic Means
f. C of 2003 on Electronic Communications (with special attention to § 155)
g. Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioral Advertising
h. Recommendations of the Hungarian National Authority for Data Protection and Freedom of Information

Budapest, 24 of May 2018

ProofIT Informatics Kft.