Data Protection and Privacy Policy
Netpositive Ltd. / netpositive.hu

Valid from: 1 January 2024

1. Introduction

Netpositive Ltd. (registered seat: 2021 Tahitótfalu, Pataksor u. 48., headquarters: 1031 Budapest, Záhony u. 7., postal address: 1031 Budapest, Záhony u. 7., company registration number: 13-09-104997, EU VAT nr: HU12643565, email: info@netpositive.hu, website: netpositive.hu, represented by Dr. Matyas Török, CEO), hereinafter: "Data Controller" complies with the following policy (hereinafter: "Policy") when processing and protecting personal and other data.
The purpose of the displayed rules is that the rights, fundamental freedoms and the right to protection of privacy is respected when processing personal data.

Data Controller declares that its data processing activities are carried out – by implementing appropriate internal policies and technical and organisational measures – at all times in conformity with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter: "Regulation") and with the provisions of Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Privacy Act").

Data Controller may unilaterally amend the Policy, with any such amendments taking effect upon publication at the website.

2. Purpose of the Policy

The purpose of the Policy is to establish internal rules and to provide a foundation for measures that ensure fair and transparent data processing, compliance with relevant legislation and the protection of personal and other data.

3. Scope of the Policy

The scope of this Policy extends to the processing of personal data concerning natural persons by the Data Controller.

4. Definitions

For easier identification we provide the meaning of the most important terms.

"**Personal data**" means any personal 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, location data or an online identifier.

"**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure

by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“**Data Controller**” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the Data Controller or the specific criteria for its nomination may be provided for by Union or Member State law;

“**Processor**” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller;

“**Third party**” means a natural or legal person, public authority, agency or body other than the data subject: Data Controller, processor and persons who, under the direct authority of the Data Controller or processor, are authorised to process personal data;

“**Consent**” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

5. Basic principles of processing

The purpose of data processing is typically contacting, maintaining contact, providing information, requesting information, identifying, managing and monitoring the used services; handling and dealing with individual inquiries, protecting the rights of the data subject and asserting the legitimate interests of the Data Controller.

Objectives of processing personal data:

- ensuring that Data Controller is aware of its business partner’s identity
- maintaining contact by electronic means (telephone, email)
- sending information and/or newsletters about products, services, etc.
- analysing website use and user patterns
- creating target groups for marketing campaigns

6. Methods of data processing

The Data Controller stores the data of the data subject on its own servers, on the Data Controller's computers, or in its paper-based records.

In all cases, data provision is voluntary, i.e. the data subject can freely decide whether to provide the requested personal data. If the data subject consents to it, the Data Controller processes the data in accordance with the applicable legislation and within the limits of the consent of the data subjects.

In order to avoid the unauthorized use of managed personal data and related abuses, the Data Controller applies security measures. Data Controller regularly checks its security procedures and develops them in line with technological development.

7. Legal basis of data processing

The legal basis for data processing is Article 6, paragraph 1, point a) of the General Data Protection Regulation, considering that the use of the services provided by the Data Controller is voluntary and the data subjects, by providing their personal data, enable the Data Controller to fulfill its mandate and provide the service. As part of the Data Controller's mandate, the data subjects consent to the Data Controller's handling of their voluntarily provided personal data.

The legal basis for data processing is also Article 6, paragraph 1, point b) of the General Data Protection Regulation, given that data processing is necessary to fulfill a contract in which the data subject is one of the parties, or it is necessary to take steps at the request of the data subject prior to the conclusion of the contract.

8. Scope of processed data

If the data subject has given their consent to data processing for direct marketing purposes, the Data Controller records the following personal data in order to send newsletters, offers and other direct marketing materials: e-mail address, telephone number, company, position. The legal basis for data processing is the consent of the data subject. The source of the data is the data subject, the place of data processing is Budapest. The data is stored electronically and Data Controller’s digital manager is responsible for data processing. Messages are sent by personal message, letter, email, or using an automated mail system. The Data Controller deletes the data immediately after the data subject withdraws his/her consent to data processing.

When applying for a job, the Data Controller records the following personal data of applicants for a specific position: name, place and time of birth, education data, work experience data, e-mail address, telephone number and all data or information that the data subject shares with the Data Controller during the selection process in the application materials (CV, motivation letter, etc.) and in the documents provided in connection with the interview. The legal basis for data processing is the consent of the data subject. The source of the data is the job applicant, the place of data processing is Budapest. The data is stored on paper and electronically (e-mail) and Data Controller’s HR manager is responsible for data processing. Data is stored until Data Controller decides on the person filling the given position, after which the data is deleted immediately.

If the data subject notifies the Data Controller of their intention to use the Data Controller’s services, the Data Controller records the following personal data of the data subject for the purpose of establishing and maintaining contact with them and for potential future cooperation: name, telephone number, e-mail address, field of expertise, organization, position. The legal basis of data processing is the consent of the data subject. The source of the data is the data subject, the place of data processing is Budapest. The data is stored electronically and the managing director of the Data Controller is responsible for data processing. The Data Controller stores the data until deletion is requested by the data subject and deletes it immediately after receiving the deletion request.

In order to fulfill its obligations under the law, Data Controller records the following personal data of the employees, related to their employment and generated during the establishment and existence of the employment: name, mother's name, place and time of birth, social security number, tax identification number, address, education and professional qualifications, title of job, date of commencement of legal relationship, extent of working hours, reason and duration of possible long-

term absence, citizenship, bank account number, telephone number, e-mail address, knowledge of foreign languages, Hungarian Standard Classification of Occupation (FEOR) number, medical fitness, assignment to a task outside the scope of work, additional legal relationship to work, disciplinary punishment, obligation to pay compensation, time of work, overtime, wages, leave, leave granted, benefits granted, debts owed by the employee to the employer, performance evaluation, development plans, evaluations. The legal basis of data processing is the fulfillment of Data Controller's legal obligations. The source of the data is the employee and the employer, the place of data processing is Budapest. Data is stored on paper and electronically and the managing director of Data Controller is responsible for data processing. Payroll-related data will be stored by Data Controller in accordance with legal provisions.

In order to fulfill its obligations under the law, Data Controller stores the following personal data of former employees, related to their employment and generated during the establishment and existence of the employment: name, mother's name, place and time of birth, social security number, tax identification number, address, title of job, the start of the legal relationship, the amount of working time, the reason and duration of any long-term absence, assignment to a task that does not belong to the scope of work, additional legal relationship for work, working time, overtime, wages, benefits given to the employee, the employee's debts to the employer.

The legal basis of data processing is the fulfillment of Data Controller's legal obligations. The source of the data is the employee and the employer, the place of data processing is Budapest. The Data Controller stores the data in accordance with the law. The managing director of Data Controller is responsible for data processing. Data is stored on paper.

In case the data subject visits Data Controller's website, in order to properly operate the website and to identify returning visitors, the Data Controller's system automatically records the following personal data of the visitor: IP address.

9. Duration of data processing

The Data Controller deletes personal data in the following cases:

- Illegal handling: in case the data is being handled illegally, the Data Controller will immediately delete it.
- Requested by the data subject (with the exception of data processing based on legislation): The data subject may request the deletion of data collected with a previous and voluntary consent of the data subject. In this case, the Data Controller will delete the data.
- The data is incomplete or incorrect and cannot be lawfully rectified, provided that deletion is not precluded by law.
- The purpose of data processing has ceased, or the statutory period for data storage has expired. The Data Controller processes the data as long as the relationship between the Data Controller and the data subject exists and as long as the Data Controller provides services to the data subject. All other data will be deleted by the Data Controller, in case it is clear that the data will not be used in the future, i.e. the purpose of data processing has ceased.

- Ordered by the court, or by the National Data Protection and Freedom of Information Authority: if a court or the National Data Protection and Freedom of Information Authority legally orders the deletion of the data, the deletion is carried out by the Data Controller. If available information suggests that the deletion would harm the legitimate interests of the data subject and in case the data subject requests it, instead of deletion, the Data Controller will block the personal data (and inform data subject about this). Personal data blocked this way can only be processed as long as the data processing purpose that precluded the deletion of the personal data exists. The Data Controller shall mark or flag personal data, if the data subject disputes its correctness or accuracy, but the incorrectness or inaccuracy of the disputed personal data cannot be clearly proven. In the case of data processing ordered by law, the deletion of data is governed by the provisions of the law. In the event of deletion, the Data Controller renders the data unsuitable for personal identification. If required by law, the Data Controller destroys the data carrier containing the personal data.

10. Entitled data processors

Based on contracts signed by the parties Data Controller transmits personal data elements to specific service providers who act as data processors, in order to fulfill their contractual obligations.

Server and network service provider
Data Controller reserves the right to involve server and network providers Magex Kft. (1133 Budapest, Váci u 76.).

Website data analysis provider
Data Controller reserves the right to involve website analysis providers Google Inc. (Amphitheatre Parkway, Mountain View, CA 94043, USA) in order to enhance the user experience of its website.

Remarketing service providers
Data Controller reserves the right to use remarketing tracking cookies and conversion pixels from providers such as Google Inc. (Amphitheatre Parkway, Mountain View, CA 94043, USA) and Facebook Ireland Ltd. (4 Grand Canal Square, Grand Canal Harbour, Dublin 2 Ireland) to present offers for products or services over the Google Content Network and via social networks.

Mailing system, direct marketing service provider
Data Controller reserves the right to use an automated mail system for sending direct marketing materials. Name of data processor: The Rocket Science Group, LLC d/b/a MailChimp (512 Means St., Suite 404, Atlanta, GA 30318, USA).

11. Data security

In respect to data processing for all purposes and legal basis, to ensure the security of personal data, Data Controller shall take all technical and organisational measures and has implemented such procedural rules as necessary for the enforcement of relevant legal provisions.

Data Controller shall apply appropriate measures to prevent accidental or unlawful destruction, loss, alteration, breach, unauthorised disclosure of, or access to, personal data.

Data Controller shall use a firewall and antivirus protection to protect the information technology system.

Data Controller shall classify and treat all personal data as confidential information. Data processed by Data Controller shall, as a rule of thumb, only be disclosed to those employees and agents of Data Controller that are engaged in implementing the data processing objectives specified in this Policy and whose contract of employment or contract of agency obliges them to confidentiality in respect to all data made known to them, in line with the legal regulations concerning their employment, or by Data Controller's instructions.

Data Controller may use the data collected from data subjects for statistical purposes, if such data is rendered anonymous – i.e., in such a manner that the data subject is not, or is no longer identifiable – in compliance with the governing legal provisions, and is entitled to publish and transfer such data to third parties.

Data Controller shall carry out electronic processing and maintain records via computer software that conforms to the requirements of data security. The software shall ensure that access to data is under purpose limitation and supervision, available only to those whose tasks necessitate such access.

In respect of automated personal data processing, Data Controller and processors shall implement additional measures designed to:

- prevent the unauthorized entry of data;
- prevent the use of automated data-processing systems by unauthorized persons using data transfer devices;
- ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data transfer devices;
- ensure that it is possible to verify and establish which personal data have been entered into automated data-processing systems and when and by whom the data were input;
- ensure that installed systems may, in case of malfunctions, be restored; and
- ensure that faults emerging in automated data-processing systems is reported.

For the purpose of protecting personal data, Data Controller shall ensure that incoming and outgoing electronic communication is monitored.

Data involved in ongoing projects and processing shall be available only to authorised employees and agents.

Data Controller shall ensure adequate physical protection of data and their relevant data carriers and documents.

Data Controller possesses adequate hardware and software tools and undertakes to implement technical and organisational measures ensuring the legality of processing and the protection of data subjects' rights

12. Rules pertaining to data processing

Data Controller, or the authorised data processor shall:

- warrant that he shall implement the technical and organisational measures ensuring compliance with relevant legal provisions, in particular in expertise, reliability and resources, including processing safety.
- ensure that in the course of its activities, the persons authorised to access data subject's personal data, unless compelled to maintain confidentiality by law, shall undertake confidentiality obligations in respect to the personal data disclosed to them.
- possess adequate hardware and software tools and shall undertake to implement technical and organisational measures ensuring the legality of processing and the protection of data subjects' rights.

13. Data Controller's rights and obligations

Taking into account the current state of science and technology and the costs of implementation, the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, Data Controller shall implement appropriate technical and organisational measures to ensure data security in line with the relevant levels of risk.

Data Controller shall take steps to ensure that any natural person acting under the authority of Data Controller who has access to personal data does not process them except on instructions from Data Controller, unless he or she is required to do so by Union or Member State law.

Data Controller shall ensure that stored data is accessible via the internal system or by direct access only to those duly authorised, and only in relation to the purpose of processing.

Data Controller shall ensure the necessary and regular maintenance and development of the equipment used. The device storing the data shall be kept in a closed room with adequate physical protections where Data Controller shall ensure physical protection thereof.

Data Controller is obliged to only engage persons with appropriate skills and expertise to carry out the tasks specified in the contract. Furthermore, Data Controller shall ensure that the persons thus engaged are trained in the applicable legal regulations on data security, the obligations described herein, and the purpose and method of data collection.

Data Controller undertakes to engage another processor only under the terms specified in the relevant legal regulations. Data Controller hereby grants general permission to its data processors to engage other processors (subcontractors). Prior to engaging another processor, a data processor shall duly notify Data Controller about the other processor's identity and the planned activities to be carried out by the other processor. In case Data Controller, based on the above information, raises objections against engaging the other processor, data processors shall only be entitled to engage another processor if the requirements specified in the objection are met.

Where a processor engages another processor for carrying out specific processing activities on behalf of Data Controller, they shall conclude a contract in writing where the contract shall apply the same data protection obligations as set out in this contract concluded between Data Controller and the processor, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfill its data protection obligations, the initial processor shall remain fully liable to the Data Controller for the performance of that other processor's obligations.

14. Data Controller's rights and obligations in case of authorising a data processor

Data Controller shall conclude a written contract with data processors for the processing activities.

Data Controller is entitled to inspect that activities carried out by data processor conform to the terms of the contract.

Data Controller shall be held liable for the legitimacy of his instructions concerning the tasks specified in the contract; however, Processor shall promptly notify Data Controller if Data Controller's instructions or the implementation thereof is against the law.

Data Controller shall be held liable for informing the natural persons in question about the processing work under this contract, and to obtain their consent if so required by law.

15. Requesting information, rights and options for legal remedy

In case of any questions or comments exceeding those contained in this Policy, Data Controller requests that data subjects contact its Data Protection Officer at the following email address: data.protection.officer@netpositive.hu

Data subjects may request information about the processing of their personal data anytime. Upon request, Data Controller shall provide detailed information concerning the data relating to the data subject, including those processed by a data processor on its behalf, the sources from where they were obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities relating to data processing, and – in case of data transfer – the legal basis and the recipients.

Data Controller must comply with requests for information without any delay, and provide the information requested in an intelligible form, in writing at data subject's request within not more than 30 days, emailed to the contact address, provided that such an email address was listed in the request. Failing that, the thirty-day time limit prescribed for Data Controller shall only be considered expired after data subject has provided their email address to Data Controller in a verifiable manner.

Furthermore, data subject may request the rectification or erasure of their personal data anytime – except data processing prescribed by law.

Data Controller informs data subject that Data Controller is obliged to erase the data in the following cases:

- if data are unlawful;
- if requested by thedata subject);
- if data are incomplete or inaccurate and lawful rectification is not possible;
- if the purpose of processing has ceased;
- if ordered by court or by the National Authority for Data Protection and Freedom of Information.

Instead of erasure, Data Controller may block personal data if so requested by the subject, or if it is assumed based on the available information that erasure is likely to violate the subject's lawful interests. Personal data thus blocked may only be processed for as long as the purpose for processing that prevented the erasure exists.

Data subject may object to processing of personal data in accordance with the provisions of the applicable law. Data Controller shall review the objection – concurrently with suspending the processing – as soon as possible, but not later than within fifteen days of the objection and shall notify the client in writing at the contact address (postal address) listed by client, provided that such contact address had been listed in client's request. Failing that, the fifteen-day time limit prescribed for Data Controller shall only be considered expired after client has provided his address to Data Controller in a verifiable manner. In case the objection is justified, Data Controller shall cease data processing, including all further data recordings and transfers, and shall block the data, and notify all parties about the objection and the measures taken on that basis to whom such objected data had been transferred and who are obliged to act to enforce the right to object. If the data subject finds the decision made by Data Controller in response to the objection questionable, data subject may bring action at a court within thirty days of having learned of the decision.

Data subject may seek ruling from a court if their rights concerning the processing of personal data have been violated. The case shall be given priority at the court. Action may be brought, as per choice, at the court of Data Controller's registered seat, or at the court of the data subject's domicile.

Data subject has the right to transparent information, which we seek to provide with this Policy.