Net.Bit ltd
IT engineering & consulting
Bul. Partizanski oderdi 18A / 3 floor 1000 Skopje
t/f +389 2 3298 533
contact@netbit.com.mk
www.netbit.mk

Data Privacy Policy

Purpose, scope and applicability

The General manager of Net-Bit is establishing this policy that prescribes the technical and organizational measures that Net-Bit as a controller and processor uses to ensure confidentiality and protection of personal data processing and to assess their adequacy with the type and scope of work processes performed by Net-Bit.

Net-Bit stands to be compliant with all relevant regulatory and legal requirements, contractual requirements and those from the international standards. Special care is taken for compliance in regards to the local Law for Personal Data Protection and EU General Data Protection Regulation (GDPR).

Net-Bit as a controller processes the following personal data categories:

- In order to implement specific labor rights and obligations, the personal data about employees: name and surname, address of residence, personal identification number and account number.
- The personal data of clients for the needs of the marketing sector for performing internal analyzes in order to determine the need to create new user packages, new marketing campaigns, etc., as well as keeping records of visitors in the Datacenter specifically: name and surname, ID card or passport number, the services that client uses, customer payments, technical data (e.g. IP address, MAC address).
- The personal data of clients, employees and third parties processed through the video surveillance system: physical appearance of employees and physical appearance of visitors when entering the Net-Bit's premises.

Net-Bit has a role of processor of personal data for client's filling systems in cases where there is an agreement for delivery of such services and according to the defined terms in the agreement.

Purposes for which Net-Bit processes the personal data are as follows:

- for the implementation of specific rights and obligations of the controller in the field of labor law;
- keeping records of visitors in the Datacenter;
- contractual obligations;
- protection of employees, their ownership and physical security of the controller's official premises.

This policy applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Data privacy principles

- **Lawfulness, fairness and transparency** - processed lawfully, fairly and in a transparent manner in relation to the data subject;

- **Purpose limitation** - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- **Data minimization** - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- **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;
- **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;
- **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;
- **Accountability** - the controller shall be responsible for, and be able to demonstrate compliance with defined principles.

Technical and organizational measures

To ensure the confidentiality and protection of the processing of personal data, Net-Bit applies appropriate technical and organizational measures to protect against accidental and illegal destruction of personal data, data loss, modification, unauthorized disclosure or access, especially when processing involves transmission of data through the network, and protection against any illegal forms of processing, as follows:

- The personal data can be processed only by authorised persons.
- Each authorized person has his own unique username and password for access to the system.
- The activities of the authorized persons are automatically registered.
- Password created by the authorized person, minimum eight alphanumeric characters long with minimum one uppercase character and minimum one special character.
- Username and password that allows the authorized person access to the information system in general and to individual applications.
- Automated log-out after inactivity of minimum 15 minutes.
- Automated lock-out after three unsuccessful log-in attempts, i.e. using incorrect username or password, and automated notification for contacting the system administrators.
- End to end encryption "Data at rest, Data in Use and Data in Motion" using security protocols as HTTPS, SSL, TLS, FTPS, ipsec.
- Firewall between the information system and the internet or any other form of external network, as a protection measure against unauthorized or malicious attempts to access or hack the system.
- Effective and secure anti-virus and anti-spyware protection, which will be constantly updated for the prevention of unknown and unplanned threats from new viruses and spyware.
- Effective and reliable anti-spam protection for the e-mail server, which is updated automatically once a day, for preventive protection against spam.
- Connecting the information system (computers and servers) to the power system using uninterruptible power supply (UPS), which will be a secondary mechanism, in case of power outage.
- Limited access to personal data and access identification.
- Destruction of documents after the expiration of data retention period is performed with a shredder device in a manner and according to the Procedure for destruction of documents, as well as destruction, deletion, cleaning and transfer of media.
- Measures for physical security of the working premises and information and communication equipment where the personal data are collected, processed and stored by using magnetic cards in combination with a code.

- Adherence to the technical instructions, when installing and using information communication equipment on which personal data is processed, which are determined in more details in the internal instructions of Net-Bit.

The servers with which Net-Bit Datacenter provides service are physically located in a separate room. The room also features special measures that reduce the risk of potential threats, including theft, fire, explosion, smoke, water, dust, vibration, chemical influences, power outages and electromagnetic radiation.

The personal data porcessed by by Net-Bit, may be disclosed only by order of the authorities, for the purposes of special investigations carried out by the authority, in accordance with the positive legal regulations.

Persons who are employed or engaged by the Net-Bit, are introduced with the regulations on protection of personal data and documentation for technical and organizational measures.

Persons who are employed or engaged by Net-Bit, before they start to work, they personally sign a Statement of confidentiality and protection of personal data processing. With the Statement of confidentiality and protection of personal data processing they undertake to adhere to the principles of personal data protection, that they will process the personal data in accordance with the documentation for technical and organizational measures to ensure confidentiality and protection of personal data processing, unless otherwise provided by law, and that they will keep the personal data confidential.

Net-Bit continuously informs the authorized persons about the direct obligations and responsibilities for personal data protection.

Data subject rights

The data subject has the right to obtain from Net-Bit as a controler confirmation as to whether or not personal data concerning him or her are being processed. Net-Bit will provide a copy of the personal data undergoing processing. At the request of the data subject, the Net-Bit as a controller is obliged to rectify, delete or restrict the use of personal data, if the data is incomplete, incorrect or not updated and if their processing is not in accordance with the provisions of the Law for Perosna Data protection.

Internal control

The system for personal data protection including the information system and information infrastructure is subjest of annual internal audit documented in Internal Audit Report. The Internal Audit Report contains the data and facts on the basis of which the opinion has been prepared and the measures for elimination of the the identified errors and shortcomings have been proposed.

The Personal data protection officer is obliged to analyze the findings of the Internal Audit Report and submit proposals to the management of Net-Bit to take the necessary corrective or additional measures to eliminate the identified errors and shortcomings.

The Internal Audit Report is available for inspection by the Directorate for Personal Data Protection.

Skopje, 28.06.2018

Net-Bit General manager