Appendix № 2

PERSONAL DATA PROTECTION POLICY
FOR THE PERSONAL DATA PROCESSED BY BILOT EOOD
Approved with Order of the Manager of BILOT EOOD dated 18 May 2018

CONTENT

I. PURPOSE AND SUBJECT MATTER OF THE POLICY. DEFINITIONS 3

II. MAINTAINED PERSONAL DATA FILING SYSTEMS.....5

III. TECHNICAL AND ORGANIZATIONAL PROTECTION MEASURES 9

IV. SPECIAL RULES FOR PROCESSING OF SENSITIVE PERSONAL DATA 11

V. PROCEDURE FOR TRACKING THE NECESSITY OF DATA PROCESSING AND THE PERIODS FOR THEIR STORAGE. RESPONSIBLE PERSONS 13

VI. PROVISION OF OBLIGATORY INFORMATION TO THE DATA SUBJECTS. RESPONSIBLE PERSONS 14

VII. RIGHTS OF THE PERSONAL DATA SUBJECTS AND THE PROCEDURE FO THEIR REALIZATION. RESPONSIBLE PERSONS 14

VIII. PERSONAL DATA PROTECTION IN UPON INCIDENTS. PROCEDURE FOR REPORTING AND MANAGEMENT OF INCIDENTS. REACTION UPON PERSONAL DATA SECURITY VIOLATION 16

IX. DESTRUCTION OF THE PERSONAL DATA AFTER THE ACHIEVEMENT OF THE PROCESSING PURPOSES 18

I. PURPOSE AND SUBJECT MATTER OF THE POLICY. DEFINITIONS

The present policy (the Policy) is developed and approved in compliance with the obligations of BILOT LIMITED, UIC 121305741, having its seat and registered address at: 88 Bulgaria Blvd., entr. 1, fl. 2, ap. 7, Vitosha Region, 1680 Sofia (hereinafter referred to as Bilot or the Company), set forth in the effective Bulgarian and European legislation in the field of personal data protection, including but not limited to Regulation (EU) 2016/679 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 (hereinafter referred to as the Regulation or the GDPR), the Personal Data Protection Act and the subordinate legislation on its implementation, as well as in addition to the Internal Rules for personal data protection, adopted by Bilot.

1.1. Purpose and Subject Matter of the Policy

The Policy`s purpose is to regulate:

1) The principles, which should be respected upon the personal data processing by Bilot;
2) Definitions of main terms with regard to the processing of personal data;
3) The maintained by Bilot registers of personal data in its capacity as personal data controller;
4) The legal grounds for personal data processing in the course of the business activity performed by Bilot;
5) The categories of data subjects, whose personal data are collected and processed;
6) The relations with third parties, to whom the processed personal data may be provided;
7) The persons responsible for the personal data processing;
8) The periods, for which the processing is performed, as well as the procedure for regular verification of the compliance of these periods;
9) The adopted technical and organizational measures and means for protection of the personal data processed by Bilot;
10) The information provided to the data subjects regarding the rights they are entitled to with regard to the processing of their personal data, as well as the procedures for the exercise of these rights;
11) The procedure in case of breach of the security of the processed personal data;
12) The procedures for destruction of the processed data on paper and on electronic media after the expiry of the periods for their storage and/ or the dropping out of grounds for their processing
13) The procedure regarding the performance of a regular verification and update of the information about the maintained personal data filing systems, incl. of the grounds of processing and the measures for protection of personal data.

1.2. Main Processing Principles

When performing all actions, processes and procedures, regarding the collection and processing of personal data Bilot respects the following main principles, set forth by the Regulation:

1) **Lawfulness, fairness and transparency** – the personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject;
2) **Purpose limitation** – the personal data are collected for specific, explicit and legitimate purposes and are not processed subsequently in a manner, incompatible with these purposes;
3) **Data minimisation** – the processed data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4) **Accuracy** – the personal data are accurate; upon necessity to be kept up-to-date every reasonable measures are taken to ensure the due erasure or rectification of the inaccurate personal data;
5) **Storage limitation** – the personal data are kept for a period no longer that the necessary for the purposes, for which the data are processed;
6) **Integrity and confidentiality** – the personal data are processed in a manner that ensures appropriate security level of the personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage, using the appropriate technical and organizational measures;
7) **Accountability** – the compliance of the abovementioned principles upon processing can be dully proved.

1.3. Definitions

Within the meaning of the present Policy and in compliance with the Regulation`s content:

1) **Personal data** means any information relating to a natural person, who is identified or identifiable directly or indirectly on the basis of a specified identifier and/ or through one or more factors specific to his/ her identity.
2) **Special categories of personal data or sensitive personal data** means personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data, biometric data, when the processing is only for the purposes of identification of a natural purpose, data concerning the health status, data regarding the sex life and/ or sexual orientation of the natural person.
3) **Data subject** means any natural person, who can be identified directly or indirectly, more specifically though an identifier such as name, identification number, location data, online identifier or through one or more factors specific to the physical, physiological, genetic, psychic, mental, economic, cultural or social identity of that natural person.
4) **Personal data processing** means any operation or set of operation, which is performed on personal data or on sets of personal data by automated or other means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making the data available, alignment or combination, restriction, erasure or destruction.
5) **Personal data filing system** means any structures set of personal data, which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.
6) **Personal data controller** means any natural or legal person, public authority, agency or other structure, which alone or with others, determines the purposes and means of the personal data processing.

7) **Personal data processor** means any natural or legal person, public authority, agency or other structure, which processes data on behalf of the controller.
8) **Personal data recipient** means natural or legal person, public authority, agency or other structure, to which the personal data are disclosed, whether a third party or not. Within the meaning of this definition, public authorities, which may receive personal data in the framework of a particular inquiry in accordance with the European Union and/ or Member State law shall not be regarded as recipients.
9) **Security violation of the personal data** means security violation, which leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
10) **Supervisory authority** means an independent public authority, burdened by the respective Member State of the EU with the responsibility to monitor the application of the Regulation with view of the protection of the main rights and freedoms of the natural persons with regard to the processing of personal data, which for the Republic of Bulgaria is the Personal Data Protection Commission.

II. MAINTAINED PERSONAL DATA FILING SYSTEMS

Bilot processes personal data in its capacity as controller, in the filing systems, as specified hereinbelow and described in details in Appendix No 2 "Filing System of the Processing Activities in the Capacity as Data Controller" to Bilot`s Internal Rules for personal data protection. The filing systems are structured with view of:

- The categories of processed personal data;
- The categories of natural persons, whose data are processed;
- The grounds and purposes of the personal data processing;
- Responsible persons with provided access to personal data;
- Periods for processing and storage and others.

2.1. Types of Filing Systems

Bilot in its capacity as data controller maintains the following filing systems with personal data:

1) **Filing System Clients** – personal data of clients – natural persons, legal representatives of clients– legal persons and their proxies, as well as of clients` employees, specified as a contact persons.
2) **Filing System Counterparties** – personal data of counterparties – natural persons, legal representatives of counterparties –legal persons and their proxies, as well as of counterparties` employees, specified as contact persons;
3) **Filing System Personnel –** personal data of employees, people working for the Company under a civil agreement, members of their families, as well as of the Managers of the Company;
4) **Filing System Job Applicants** – personal data, collected and processed in the course of the Company`s personnel selection;

5) **Filing System Accounting** – personal data of employees and contractors, working for the Company under a civil agreement; Manager; counterparties and clients, legal representatives of counterparties and clients, their proxies and employees, incl. contact persons; legal representatives/ proxies of the sole owner of the capital of the Company;
6) **Filing System Company Status** – personal data of the Manager and its proxies, as well as of the legal representatives of the sole owner of the capital and their proxies, contained in documents, concerning the legal status of the Company;

2.2. Grounds for the Processing of Personal Data by Filing Systems

1) **Art. 6, paragraph 1, letter a):**
   - on the ground of the explicit consent of the subjects – upon organization of business trips in the country and abroad, with regard to performance of internal communication on non-business occasions, as well as for provision of additional acquisitions to the personnel;
2) **Art. 6, paragraph 1, letter b):**
   - with view of the performance of its obligations under the agreement, concluded with the data subject;
   - undertaking steps for conclusion of an agreement upon request of the data subject.
3) **Art. 6, paragraph 1, letter c):**
   - for the fulfillment of the obligations of the Company pursuant to the Bulgarian legislation;
4) **Art. 6, paragraph 1, letter f):**
   - for protection of the legitimate interests of the Company – comprising in performance of the business activity of the Company;
   - after termination of the respective agreement part of the data are processed for protection of the legitimate interests of the Company – with regard to potential inspections and/ or claims, concerning the contractual relations.
5) Art. 9, paragraph 2, letter b):
   - for the fulfillment of the Company`s obligations pursuant to the Bulgarian legislation in the field of social security and social protection;
6) Art. 9, paragraph 2, letter h):
   - for the purposes of the preventive or occupational medicine and assessment of the work capacity of the employee/ contractor.

2.3. The Consent as a Ground for Personal Data Processing

Upon necessity and when this is permissible by the Regulation and the effective legislation, the Company processes personal data as a controller as well on the ground of the explicit written consent of the data subject regarding such processing.

When the Company processes personal data on the grounds of consent of the data subjects, it ensures that the consent is provided and that it is compliant with the requirements of the GDPR, and namely:

- the consent is clearly distinguishable, when it is part of another document;
- the consent contains clear and unambiguous information regarding the purposes and periods for processing of the personal data;

- the data subjects are provided with the opportunity to provide separate consent for the different purposes for processing;
- the subjects are informed for the opportunity to withdraw their consent at any time and are provided with an easy way to do so;
- the fulfilment of an agreement/ provision of a service is not conditional upon the provision of the consent for processing, when the latter is not necessary for the fulfilment of the agreement/ provision of the service.

When the consent relates to the processing of personal data of a person, under the age of 14, it is provided by the legal representative of that person – parent or guardian. When the consent relates to the processing of personal data of a person over 14 years of age but under the age of 18, it is provided by the child and by a parent/ trustee.

Upon withdrawal of the consent, the collected personal data are destroyed in compliance with the terms and conditions of Section IX of the present Policy, unless Bilot assesses that legitimate interest or incurred statutory obligation to store the data for a specific period. The withdrawal of the consent does not affect the lawful data processing up to the moment of the withdrawal.

2.4. Access and Storage

The personal data collected and processed by Bilot in its capacity as personal data controller are stored on electronic or paper media.

Different organization of the access to documents containing personal data and different procedures for work with the data are established for the different filing systems.

Access to the processed and stored personal data on paper and/ or electronic media is provided to the persons, specified in column "Responsible persons with provided access to the personal data from the filing system" for each filing system, pursuant to Appendix No 2 to Bilot`s Internal Rules for personal data protection and, in accordance with the terms and conditions of the present Policy. The personal data may be provided as well to the persons specified in column „Categories of possible recipients of personal data" for each filing system, pursuant to Appendix No 2 to Bilot`s Internal Rules for personal data protection, on the basis of a contractual or statutory obligation.

When accessing the personal data from the respective filing system the established for the register technical and organizational measures are complied with, as they are described in Section III of the present Policy.

The periods for storage of personal data in the separate filing systems are different depending on the different grounds and purposes for the processing. The periods for each filing system are specified in Appendix No 2.

2.5. Responsible Persons with Regard to the Personal Data Processing

The personal data processing within the frameworks of the Company is assigned to the persons, who are provided with access to the personal data, processed in the respective filing system and who are familiar with the specific requirements of the Regulation, the Personal Data Protection Act and the present Policy with regard to the processing and storage of personal data, incl. of sensitive personal data.

In particular, for each filing system they are listed exhaustively in Appendix No 2 to Bilot`s Internal Rules for personal data protection.

2.6. Relations between controller and processor of personal data

In the cases when the Company in its capacity as controller assigns the processing of specified personal data to a third party – data processor, the relations with the processor are regulated by a written act (agreement), which details the processor`s obligations in compliance with the Regulation and the relevant national legislation, incl. the application by the latter of appropriate technical and organizational protection measures. Before the conclusion of the agreement the Company investigates the third party, to whom the data processing will potentially be assigned, in order to be assured that this person possesses expert knowledge, reliability and resources, and upon such assignment enough guarantees will be present for the protection of the personal data subjects and their lawful processing.

For that purpose the employee responsible for the conclusion of the agreement with the processor, undertakes and documents the performance of the following actions: verifies the reputation of the processor through the publicly available forces of information; requires the internal acts regarding the data protection adopted by the processor and evidence, for the way the processor`s employees are engaged with their compliance; requires information for the used software for data processing, as well as for the other implemented measures technical and organizational measures for data protection.

The Employee responsible for the conclusion of the agreement with a processor monitors the written act (agreement) between the Company and the processor to be compliant with the requirements of the Regulation. The agreement is coordinated with the employee designated by the Company.

2.7. Provision of Personal Data to Third Parties

The personal data collected and processed by Bilot in its capacity as controller may be provided to the following (categories of) persons:

A) With respect to the personal data processed by Bilot in its capacity as controller, contained in the filing systems under Section II, Art. 2.1, hereinabove, an obligation for their provision to the competent authorities may occur, in fulfilment of obligations of the Company, arising from the effective legislation – such as **National Social Security Institute, National Revenue Agency, "General Labour Inspectorate" Executive Agency, State Agency "National Security", Personal Data Protection Commission, Commercial Register, bodies and officers of the Ministry of Interior, court, prosecutor's office** etc.

B) Personal data are processed **by providers of different services** to the Company, ensuring its business activity, such as: the auditor of the Company; lawyers and other consultants of the Company and others (third parties – processors), on the basis of the agreements concluded with the Company, in compliance with the specified in Art. 2.6. hereinabove, with regard to the fulfilment of statutory and contractual obligations of the Company, connected with the relation with the data subject (incl. to ensure health and safety at work), as well as for the protection of the legitimate interest of the Company in the course of its activity, as they are specified for each Filing system in Appendix No 2 to Bilot`s Internal Rules for personal data protection:

2.8. Joint Controllers

In the cases when the Company and a third party jointly define the purposes of personal data processing they are joint controllers with respect to the processed personal data. The relations between the joint controllers are regulated by a written act (agreement), which details the obligations of each of them in compliance with the Regulation and the relevant national legislation and in particular it settles the obligations of the parties in connection with:

- the exercise of the rights by the data subjects;

- the provision of information to the data subjects;
- the roles and relations of the joint controllers to the data subjects.

The significant characteristics of the reached agreement, including the joint contact person with the data subjects, if the joint controllers have designated such, are provided to the data subjects. Regardless of the reached agreement, the data subjects can exercise their rights under the Regulation and the applicable national legislation towards each of the joint controllers.

In case between the joint controllers such agreement has not been reached, the processing of the personal data by each of them is settled in accordance with the adopted internal acts, including, but not limited to, Personal Data Protection Policy Internal rules and procedures, General terms and conditions and others with regard to the personal data processing, in compliance with the requirements of the Regulation and the relevant national legislation.

2.9. Provision of Personal Data outside the EEA and Switzerland

Bilot does not provide personal data to third parties outside the European Economic Area (EEA) and Switzerland.

2.10. Information Update Procedure by Filing Systems

Upon necessity, but not less than once a year, until March 31th of the respective year, Bilot`s employees, to whom the processing of the collected personal data is assigned, under the guidance and supervision of Chief Accountant verify whether any factual change has occurred in the processing activities, performed in the filing systems under Appendix No 2 to Bilot`s Internal Rules for personal data protection (incl. in the grounds, purposes, the processed data, the subjects, the recipient etc.) and whether such is necessary due to legislative changes or other reasons.

The results from the conducted verification are documented through a written protocol, containing ascertainment and recommendations for actions. In case the necessity to implement alterations in the regulation of the processing activities in the filing systems is ascertained, actions of the adoption of the respective alterations in the present Policy shall be undertaken.

III. TECHNICAL AND ORGANIZATIONAL PROTECTION MEASURES

3.1. General Principles for Implementation of Protection Measures

In its capacity as controller Bilot performs a regular evaluation of the risks for the rights of the subjects, connected with the personal data processed by it, and implements and applies appropriate technical and organizational measures to ensure that it is able to provide the lawful personal data processing on the grounds and for the purposes, for which it is performed, including – that by default the data are not accessible for unlimited number of natural persons (**data protection by default**)

When choosing, introducing and/ or implementing new software products, configurations and systems, related to the personal data processing, the Company, taking into account the achievements of the technical progress, the expenses on the implementation of the new software products, configurations and systems, as well as the risks of the data processing for the rights of the subjects, takes into account that they should additionally ensure yet at the design stage (**data protection at the design stage**) that:

- the processed personal data are kept to minimum – only personal data that need to be processed for the stated purposes are processed;

- the personal data are accessible only for the necessary number of persons with view of the stated processing purposes;
- transparency regarding the functions and the personal data processing is present;
- applications and processes that allow the implementation of appropriate data protection measures are used.

3.2. Types of applied protection measures

With respect to the personal data collected and processed by the Company in its capacity as controller, the following technical and organizational personal data protection measures are adopted and implemented:

1) **Physical protection of the personal data**, implemented through:
   - Storage of the personal data on paper in locked cabinets/ locked premises, located in area with controlled access;
   - Limited access to the office premises. Locking the office premises during non-working hours and security through a mounted security system with access code;
   - Fire alarm system (fire signal system) and fire extinguishing media;
   - Video surveillance and physical security of the building, in which the office premises of the Company are located.
2) **Organizational and administrative** – regulation rules with regard to the processing of personal data in the adopted internal rules, procedures and acts of the Company;
3) **Logical protection** regarding the personal data stored on electronic media – Firewall (FW), Antivirus (AV);
4) **Logical protection** regarding the personal data stored on electronic media, on the working stations (personal computers) of the separate employees, to whom the personal data processing in practice is assigned, – FW, AV;
5) **Maintenance of the antivirus programs** – ESET NOD32
6) **Controlled access** to the personal data stored and processed on electronic media on the basis of the following criteria – limited administration of the user accounts, preliminary set access level, user name and password for access, remote access, IP, department, position, logical group, employee, time period;
7) **Maintenance of an electronic archive in NAS – Network Attached Storage with mirror discs (data protection)** and regular weekly archiving of the information databases, containing personal data;
8) **Keeping records (logs) of at least the following processing operations:** collection, alteration, references, disclosure, including transfer, combination and erasure, which provides the opportunity for determination of the ground, date and time of such operations and as far as it is possible — identification of the person, who has made the reference of has disclosed personal data, as well as data identifying the recipients of these personal data;
9) **Remote access protection –** installed program for remote access Team Viewer, which is used for the purposes of the technical maintenance and in case of problems with the accounting software, as during its use the process is always supervised by a Company`s employee.

10) **Ensuring the fulfilment the undertaken confidentiality obligations**, by undertaking obligations by personal data processors, as well as by the employees and contractors under civil agreements, working in the Company, through their inclusion in the agreements concluded with the respective persons or the attached documents, as well as assignment of obligations with regard to the processing of personal data, undertaking a confidentiality engagement in the job description of the employees, to whom the processing of personal data is assigned and obligation for compliance with the internal personal data protection acts of the Company;
11) **Archiving and Inventory of documents on paper**, from the specified hereinabove filing systems containing personal data, as well as access limitation to the archived data only for authorized persons, in accordance with the terms and conditions of the present Policy;
12) **Electronic signature**, which is connected to the computer only when it is used;
13) **Encryption and regular formatting** of the flash memory sticks, which are used in the Company.

3.3. Procedure for verification of the compliance with the applied security measures. Measures update.

1) With view of minimizing the risks connected with the personal data processing, and in particular – from accidental and unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data, the Company performs a regular testing, appraisal and evaluation of the effectiveness of the applied technical and organizational measures.
2) Upon performance of that appraisal on a sample basis is tested the factual compliance of the established in the present Policy measures by the persons processing personal data in the filing systems in accordance with Appendix No 2 to Bilot`s Internal Rules for personal data protection.
3) The verification regarding the applied measures and the appraisal of their effectiveness and u topicality is performed regularly, but not less than once a year until March 31th of the respective year, by Chief Accountant
4) The results from the performed verification are documented through a written protocol containing statements and recommendations. In case the necessity to implement new protection measures is stated, the respective alterations in the present Policy are initiated.

IV. SPECIAL RULES FOR PROCESSING OF SENSITIVE PERSONAL DATA

4.1. Grounds for the processing of sensitive personal data

The collection and processing of special categories personal data (sensitive data) as a rule is performed by Bilot in its capacity as controller – when this is necessary for the purposes of the fulfilment of the obligations and the exercise of the special rights of the Company or of the data subject by virtue of the Labour law, for the purposes of the preventive or labour medicine (through assignment to Occupational health service, bounded by obligation by law to keep confidentiality) or in other cases explicitly permissible by the Regulation and/ or the effective legislation (including via assignment to a third party – data processor, in compliance with Art. 2.6. of the present Policy).

4.2. Additional protection measures upon processing of sensitive personal data

When processing sensitive personal data Bilot ensures the application of stricter measures for their protection (including upon receipt/ submission of the information and upon its subsequent processing and storage) with view of ensuring appropriate guarantees for the rights of the data subjects

In case of automated processing of sensitive data Bilot in its capacity of personal data controller, after performed evaluation of the risks for the rights of the data subjects, applies measures, aiming to provide:

1) control over the access to equipment (unauthorized persons to be denied access to the equipment used for the processing);
2) control over data media (unauthorized persons to be prevented from reading, copying, alteration or removal of data media);
3) control over storage (unauthorized persons to be prevented from entering personal data, as well as conduction of verifications, alteration or removal of stored data by unauthorized persons);
4) control over users (unauthorized persons to be prevented from using the information system of the Company through using the equipment for data transfer);
5) control over data access (to be ensured that persons authorized to use of the information system of the Company, have access only to the personal data, covered by their access authorization);
6) control over communication (to be ensured opportunity for verification and determination to which bodies have been or can be transferred data through equipment for transfer of data);
7) control over data entry (to be ensured the opportunity for subsequent verification and determination what personal data have been entered into the information system of the Company, as well as when and by who these personal data have been entered);
8) control over transfer (unauthorized persons to be prevented from reading, copying, alteration or removal of personal data when transferring of personal data or their transport on data media);
9) restoration (to be ensured the opportunity for restoration of the installed systems in case of failure of the systems` functions);
10) reliability (to be ensured the performance of the functions of the information system and the report for occurred function defects);
11) integrity (to be ensured that the stored personal data are prevented from damage due to malfunctioning of the information system).

In particular, in addition to the security measures, described in Section III hereinabove, Bilot applies as well the following measures:

- In all cases of transfer/ transport of information by electronic means and/ or electronic media the personal data are protected by information encryption at the starting point of the transfer/ transport and its decryption at the end point, including by use of password, encryption program or electronic signature.
- Access to the stored sensitive personal data is performed only by the persons with provided access in accordance with this Policy and Appendix No 2 to Bilot`s Internal Rules for personal data protection.

- The storage of sensitive personal data on other electronic media, other than the device NAS, in the directories, specifically determined for storage of these data, is not allowed. Regularly (every 6 months) Chief Accountant performs a verification whether local copies of the processed documents containing sensitive personal data, are stored on the hard disks of the personal computers of the employees with granted access to these data. When such are present, they are copied on the NAS, and the local copies are destroyed in accordance with the procedure specified in Section IX, Art. 9.2. of the present Policy.
- The sensitive personal data on paper are stored only in locked cabinets, located in area with controlled access.
- In case of physical transport of sensitive data collected and/ or stored on paper, they are placed in sealed opaque envelopes with sign „Strictly confidentially".

V. PROCEDURE FOR TRACKING THE NECESSITY OF DATA PROCESSING AND THE PERIODS FOR THEIR STORAGE. RESPONSIBLE PERSONS

In fulfilment of its obligations as personal data controller and with view of the application in practice of the principles of the GDPR, and in particular the principles of lawfulness, fairness and transparency of the processing, limitation of the purposes and of the storage, data minimization and accountability of the processing activities, the personal data collected and stored by Bilot are subject to regular verification regarding the necessity of their further processing and the periods for their storage. The personal data are stored for a period no longer than the necessary for the purposes, for which they are processed, resp. the provided by law.

At the end of every 6 month period of the current calendar year, the employees of Bilot provided with access to the collected personal data, under the guidance and supervision of Chief Accountant, verify the personal data processed and stored by the Company on paper and electronic media with view of the presence of necessity for their further processing and tracking of the periods for their storage. The results from the conducted verification are documented through a written protocol, prepared by Accountant.

In case that with regard to certain personal data it is determined that, the necessity for their processing has ceased and/ or that the purpose, for which they have been collected is fulfilled, and/ or that the storage periods, as defined in Appendix No 2 to Bilot`s Internal Rules for personal data protection for the respective filing system, are expired, they are destroyed in accordance with the set forth in Section IX hereinbelow.

Upon expiry of the storage period for the personal data from the respective register, as specified in Appendix No2 to Bilot`s Internal Rules for personal data protection, the personal data are marked as subject to destruction and are destroyed in accordance with the set forth in Section IX of the present Policy after CEO is dully notified for these circumstances.

VI. PROVISION OF OBLIGATORY INFORMATION TO THE DATA SUBJECTS. RESPONSIBLE PERSONS

6.1. Requirements to the Provided Information

In fulfilment of the principle of lawfulness, fairness and transparent personal data processing towards the subjects, in each case of personal data processing in its capacity as controller Bilot provides to the data subjects specific information for the performed processing, which:

1) is in short, understandable and easily accessible form;
2) is prepared in clear and plain language;
3) clarifies:
    - the legal ground and the purposes of the processing;
    - the source of the personal data (if it is different than the subject itself);
    - the data recipients of categories of recipients;
    - possible provision of the data to a third country;
    - period of the processing;
    - rights of the natural persons.

6.2. Periods for Provision of the Information

The information is provided to the persons within the following periods:

- Upon receipt of the personal data by the data subject – at the moment of their receipt;
- Upon receipt of the personal data from another source – within a reasonable period after that, but no longer than 1 month, unless the first contact with the data subject or their first transfer to another recipient takes place earlier (in which case the provision of the information is conducted at latest at the first contact/ transfer to another recipient).

6.3. Responsible Persons for the Provision of the Information

The persons responsible for the provision of the information to the subjects, whose data are processed, are the persons with granted access to the personal data from the respective filing system in accordance with Appendix No 2 to Bilot`s Internal Rules for personal data protection, under the supervision of Chief Accountant.

VII. RIGHTS OF THE PERSONAL DATA SUBJECTS AND THE PROCEDURE FO THEIR REALIZATION. RESPONSIBLE PERSONS

In order to ensure the protection of the interests of the personal data subjects and the security of the processed personal data they have to rights explicitly regulated by the GDPR, to which correspond certain obligations of the personal data controllers.

7.1. Rights of the Personal Data Subjects

The data subjects are entitled to:

1) **Access right** to the processed personal data – the data subject is entitled to receive a confirmation by the controller whether personal data relating to him/ her are processed – to be provided with access to the data and to specific information regarding the processing;

2) **Right of rectification** of the personal data – the data subject is entitled to request the controller to rectify without unnecessary delay the inaccurate personal data about him/ her;
3) **Right of erasure** (right "to be forgotten") – the data subject is entitled to request by the controller the erasure of the personal data related to him/ her without unnecessary delay, in certain hypotheses specified in the GDPR;
4) **Right of limitation of the processing** – the data subject may request limitation of the processing in certain hypotheses specified in the GDPR. I these cases the processing can be performed only with the consent of the data subject or for the determination, exercise or protection of legal pretensions or for the protection of the rights of another natural person;
5) **Right of data portability** – the data subject is entitled to receive the personal data which concern him/ her and which he/ she has provided to the controller, in structured widely used and machine-readable format, as he/ she is entitled to transfer these data to another controller. The subjects are entitled to these rights when: 1) the processing is on the ground of a consent or contractual obligation, and 2) the processing is performed in an automated manner;
6) **Right of notification for violation of the security of the personal data** – the data subject is entitled to be notified for the occurred violation of the security of his/ her personal data, when there is a possibility that violation to cause high risk for the rights and freedoms of the concerned data subject;
7) **Right of objection** – the data subject is entitled at any time to object against the processing of data concerning him/ her, when the processing is performed with view of the protection of the legitimate interests of the controller or third party;
8) **Right of withdrawal of the consent for processing** – the data subject is entitled to withdraw the provided consent for processing at any time, as that does not affect the lawfulness of the processing performed up to that moment on the ground of the prior consent;
9) **Right of claim to supervisory authority** – the subject is entitled to file a complaint against the controller and/ or processor with regard to the performed processing of his/ her personal data;
10) **Right of judicial remedy** – the data subject is entitled to undertake the necessary actions for realization of his/ her judicial remedy against the obligatory decision of supervisory authority concerning him/ her, as well as against actions of the controller and/ or processor on processing of his/ her personal data, violating his/ her rights under the Regulation, in the manner provided for such protection in the Regulation and/ or the effective legislation.

7.2. Procedure for Exercise of the Rights under Art. 7.1, it. 1-8

The rights under it. 1-8 hereinabove, shall be exercised by the data subject by submitting a written request to the Company at the following address: 88 Bulgaria Blvd., entr. 1, fl. 2, ap. 7, Vitosha Region, 1680 Sofia**.**

The request can be submitted as well as through electronic means, as for that purpose an e-mail shall be sent to the following e-mail address: pacheva@bilot.bg; bogomilova@bilot.bg;

When the request is submitted by electronic means, the information with regard to it is provided as well by electronic means, unless the data subject has expressly requested otherwise.

Information for the undertaken activities with regard to the request is provided to the data subject in writing (incl. by e-mail), without unnecessary delay at latest within 1 (one) month period as of its receipt by the Company.

Taking into account the complexity and the number of the requests, the Company can extend the period for provision of the information regarding the undertaken activities with a maximum of 2 (two) additional months. For each such delay the Company informs the data subject within 1 (one) month of the receipt of the initial request, specifying as well the reasons caused the delay.

After consideration of the complaint with view of the necessary actions for his/ her satisfaction and potential inability for their conduction and/ or excessiveness of the efforts in this regard, the Company may not undertake actions with regard to the request of the data subject. In this case Bilot notifies the data subject for that without unnecessary delay and at latest within 1 (one) month of the receipt of the requests, stating as well the reasons, due to which Bilot will not undertake actions for its satisfaction. In this regard, the data subject is notified for the opportunity to file a complaint to a supervisory authority and/ or to seek judicial remedy, in accordance with the rights specified in it. 9 and it. 10 hereinabove.

7.3. Procedure for Exercising the rights under Art. 7.1, it. 9

The supervisory authority competent to examine the submitted complaint with regard to the processing of personal data on the territory of the Republic of Bulgaria is the Personal Data Protection Commission (PDPC).

Complaints to PDPC with regard to the illegal and/ or unlawful personal data processing can be submitted by post and/ or courier at the following address: 2 Prof. Tsvetan Lazarov Blvd., Sofia 1592 , or via email: **kzld@cpdp.bg**.

7.4. Responsible Persons for the Implementation of the Procedure

After receipt of a request from the data subject, Accountant on the basis of the information regarding the processing, collected by the persons with granted access to the personal data of the subject (as specified for the separate filing systems in Appendix No 2 to Bilot`s Internal Ruled for personal data protection), prepares a draft replay and after its approval by Chief Accountant send it to the data subject, who made the request.

VIII. PERSONAL DATA PROTECTION IN UPON INCIDENTS. PROCEDURE FOR REPORTING AND MANAGEMENT OF INCIDENTS. REACTION UPON PERSONAL DATA SECURITY VIOLATION

8.1. Personal Data Protection upon Incidents

For personal data protection, the Branch has a prepared and approved recovery plan in case of disasters and breakdowns, which provides detailed information for where to go and what and when to be done in case of a disaster or catastrophe. The fundamental principle of this plan is to ensure the framework for the Company to react to any crisis occurred, regardless of whether it is foreseen or unforeseen. The plan foresees actions, which should be done before, during and after the reporting of the disaster. It includes:

- determination of the criteria, according to which the disaster (catastrophe) will be reported;

- who can report for this;
- how the responsible persons should be notified;
- what specific actions to be undertaken in order to recover the affected part of the Company`s activity after the incident;
- security measures during and after the incident;
- other relevant issues.

8.2. Procedure for Reporting and Management of Incidents

When an incident (accident, breakdown, disaster or other unforeseeable circumstance that may affect the security of the personal data) occurs the persons, to whom the data processing is assigned immediately inform Chief Accountant and the Manager of the Company, and are obligated as well to undertake all necessary measures for the prevention or limitation of the damage of the personal data filing systems. These actions are performed in compliance with all other safety requirements and without any risk for the health and life of the members of the personnel of the Company.

In case of theft or other unlawful seizure of property and information, the police authorities, the insurer, the company providing security services, as well as other competent persons are immediately notified, , if this is required by the effective legislation in view of the circumstances.

For each incident that has led to the damage of stored personal data, a protocol is prepared by Chief Accountant, and if that is impossible – by the persons directly processing the affected data, which contains: the time of occurrence of the incident and the time of its finding, the reasons for the incident, the damages caused and the undertaken measures for their limitation, as well as a recommendation for t prevention of a second incident.

In case that fault of employees of the Company is found for the occurrence of the incident, actions are undertaken for seeking the respective disciplinary and/ or civil liability in accordance with the requirements of the effective legislation.

8.3. Reaction upon Personal Data Security Violation

In case of found personal data security violation within the meaning of the present Policy and the Regulation, Chief Accountant documents in writing each personal data security violation, specifying the facts, connected to it, the consequences that have occurred and the undertaken measures and actions for coping with the violation and the consequences from it.

The Company in its capacity as controller of personal data, with respect to which the security violation is committed, notifies without unnecessary delay the PDPC, in its capacity as supervisory authority, for the committed violation, no later than 72 (seventy-two) hours as of the moment of the discovery of the violation, when possible. When the information cannot be submitted simultaneously it is submitted gradually without unnecessary delay.

The notification for personal data security violation to the PDPC shall contain at least the following information:

1) Description of the nature of the security violation and, if possible, the categories and the approximate quantity/ number of the affected personal data records and personal data subjects;
2) Description of the consequences that might arise from the committed security violation;

3) Information about the undertaken and/ or applied measures for coping with the personal data security violation and reduction of the potentially occurred from it potential adverse consequences;
4) The reasons for the delay in the submission of the notification if it is submitted after the 72-hour period.

When there is likelihood the personal data security violation to cause high risk with regard to the rights and freedoms of the concerned data subjects, the Company notifies in writing and without unnecessary delay the data subject for the committed violation.

This notification is prepared in a clear and understandable for the data subject language and includes the information under it. 1) to 4) inclusive hereinabove

Such notification to the subject may not be performed when:

1) The company has undertaken appropriate technical and organizational protection measures and these measures have been applied towards the personal data affected by the security violation (in particular the measures, which make the personal data, incomprehensible for any person, who does not have authorization for access to them, such as encryption); or
2) The Company has undertaken subsequently measures, which ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialise; or
3) The personal notification of each data subject would lead to disproportionate efforts. In such case the Company makes a public notification or undertakes other similar measure so that the data subjects are informed to an equal extent.

IX. DESTRUCTION OF THE PERSONAL DATA AFTER THE ACHIEVEMENT OF THE PROCESSING PURPOSES

After the purpose of the personal data processing is achieved and/ or after the expiry of the storage periods specified in Appendix No 2 to Bilot`s Internal Ruled for personal data protection, Bilot destroys/ erases the relevant personal data by taking adequate measures to prevent unauthorized access to the personal data during their destruction.

The determination of the personal data, which should be destroyed is performed on the basis of a verification under the control of Chief Accountant for the tracking of the necessity for personal data processing and the periods for their storage under the provisions Section V of the present Policy.

Only documents on paper and/ or electronic media containing personal data, **which are neither subject to return** to the customers/ counterparties of Bilot or to the data subjects, **nor shall be submitted** to the competent public authority in compliance with Bilot`s statutory obligation in its capacity as personal data controller (such as the National Social Security Institute), should be destroyed.

9.1. Destruction of data on paper

The destruction of personal data from different filing systems maintained by Bilot, stored and processed on paper, is responsibility of the respective employees and/ or specified persons, to whom the personal data processing is assigned and access to them is provided, pursuant to Appendix No1 to the present Policy.

The documents subject to destruction are submitted to the person, occupying the position Accountant, after the completion of the annual archiving and compiling a list of files, subject to destruction in order to organize the physical destruction of the documents. A protocol in writing shall be prepared regarding the destruction.

9.2. Destruction of data on electronic media

The destruction of personal data from different filing systems maintained by Bilot, stored and processed on electronic media is initiated by the respective employees and/ or specified persons, to whom the personal data processing is assigned and access to them is provided, pursuant to Appendix No1 to the present Policy.

The personal data stored on the personal computers, incl. personal data stored in the e-mailbox in the form of e-mails and/or attachments, are reviewed and destroyed by the respective employee, using the device.

All personal data stored and processed on portable electronic media (*CD/ DVD/ BRD/ USB Memory Stick*) and/ or hard disk on a portable or stationary computer are destroyed by the respective employee under the supervision and with the knowledge of Chief Accountant, by using the appropriate programs for that – Electronic shredders, that record unnecessary zeros and ones in place of the erased files.

The personal data stored on the NAS are destroyed by the initiation of the respective employees and/ or specified persons, to whom the personal data processing is assigned and access to them is provided, pursuant to Appendix No 2 to Bilot`s Internal Rules for personal data protection under the supervision and knowledge of Chief Accountant.

The archived databases with NAS information are destroyed by the respective employees and/or specified persons with access.

For each procedure for destruction of personal data on electronic media, regardless of whether the data are located on personal devices of on the Company`s NAS, a protocol in writing or other document is prepared.

BILOT EOOD in its capacity as personal data controller reserves its right to amend and update the present Personal Data Protection Policy and the Appendix to it at any time with view of possible changes in the personal data protection regime and the applicable European and national legislation in this field, as well as in case of changes in the performed processing and/ or the applied practices and procedures in this regard.