

## **Personal Data Protection Policy**

### **Clause 1**

#### **Company**

Green Development LLC (hereinafter the “Company”)

I/N# 204452412

Address.: #42 Avto Varazi str., 0186 Tbilisi

E-mail: [sales@ubani.ge](mailto:sales@ubani.ge)

Web-page: [www.ubani.ge](http://www.ubani.ge)

### **Clause 2**

#### **Purpose of the policy**

The purpose of the personal data protection policy is to determine the category(ies) of personal data by the company within the scope of its activity; to determine the procedure and the ground(s) for their collection, processing, storage, security/protection, transmission; to provide information to data subject; to determine the proportionality of interference with the protected area and to avoid unjustified interference, to build a corporate activity culture equipped with high level of responsibility.

### **Clause 3**

#### **Principles**

The following principles shall be observed when interfering with the personal data area:

- Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject, without infringement of his/her dignity;
- Data shall be collected/obtained only for the specific, explicit and legitimate purposes;
- Data shall be processed only in the volume necessary to achieve a relevant legitimate purpose. Data shall be proportionate to the purpose for which they are processed;
- Data shall be accurate and, where necessary, kept up to date. Given the purposes of data processing, inaccurate data shall be rectified, deleted or destroyed without undue delay;
- Data shall be kept for a period necessary for data processing for achieving a relevant legitimate purpose. Upon achieving the purpose for which the data is processed, they shall be deleted, destroyed or stored in a depersonalized form, unless the data processing/storage is determined by law and is a proportionate measure to protect the overriding interests in a democratic society;
- For security of personal data, the data shall be processed using technical and organizational measures that ensure appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

## Clause 4

### Data categories

In course of the company's activity, given the nature of the purpose and taking into account its proportionality, the processed information may include as follows:

- Identification data - full name / title, personal/identification number, ID/proof of citizenship document number, date of birth/registration and relevant document data, sample signature (including qualified electronic signature);
- Contact information– legal and/or actual residential/location address, e-mail, mobile or landline phone number, contact person(s) data (including its identity and contact channels);
- Documentary data – ID, passport, driving license, birth certificate, certificate of compatriot residing abroad, residence card, extract from the Registry of Entrepreneurs and Non-entrepreneurial Legal Entities of the National Agency of Public Registry, status-Neutral Identity Card or status-Neutral travel document number, taxpayer identification number, representative authority document etc.;
- Financial data – company's payment history, claims/obligations, payment schedule, arrears, fines, payments/transfers and their details, balances and other transaction related information;
- Technical data – information on the device applied when using the company products and other technical details, for example, Internet Protocol (IP) address, operating system, cookies, IMEI code, application logs, behavioral data, location information, information on the company's social media mobile apps, products and use of services, including ratings and survey responses;
- Audio-visual data - records of incoming/outgoing phone calls to the company's number, video and audio monitoring system records, photos;
- Marketing data – information on the subject's interests necessary for the planning and implementation of marketing activities on part of the company, including the preferred form of communication for receiving marketing notifications, content, consent etc.;
- Socio-demographic data – information related to citizenship, education, workplace, marital status etc., as well as that related to the language, gender, age, social status;
- Interaction data – data recorded in course of direct communication with the company, when filling out physical forms, on the phone, via e-mail or through other communication channels;
- Public data – data obtained from public sources, recorded in various databases and/or freely available in other sources;
- Special category data relating, for example, to criminal conviction, health, as well as biometric data, including facial features and expression, etc.,
- Marital status, information on family members – marriage certificate, family members' identification and documentary data, information on the family members, contact persons, information on person's death, death/succession certificate etc.;
- Contractual data - details of the transactions concluded (and/or having the status of pre-contractual relationship) with the company and the content thereof, to which the data subject is a party, a third party and/or representative thereof.

## **Clause 5**

### **Data subject**

The addressee circle of the personal data protection policy herein includes, but is not limited, to the following:

- state and non-state, civil, commercial, public institutions; local self-government and state bodies and the local structures/bodies/agencies/LEPLs thereof; legal and non-legal (non-commercial) entities of public or private law; individual associations and other bodies;
- company's primary and additional product users, both, contractors and subcontractors (including potential, available and/or former ones);
- company's primary and/or additional product providers, both contractors and subcontractors (including potential, available and/or former ones);
- direct participants in the delivery/transfer of the company's primary and/or additional products to another third party(ies), both contractors and subcontractors (including potential, available and/or former ones);
- contractor/subcontractor representatives (including legal representatives) or contact persons;
- direct executor persons/agencies of the controlling, registrar or other state authorities or representatives thereof;
- any individual contacting the company and showing interest in a specific product;
- individuals not directly related to the company, whose data, however, should be processed for the implementation of the company's activity or for improving the company's products;
- individuals in any way connected to the company, the company's products, and who establish contacts with it through various communication channels;
- one or more from the above-listed persons who are minors under the age of 18 – their data shall be processed in accordance with the legislation of Georgia, with due account for the best interests of the minor.

## **Clause 6**

### **Person authorized/responsible for processing**

Given the context and purpose of processing, during the data processing, the company and/or any third party (to whom the data was transferred) may serve as a person authorized to process the data and act on behalf of the person in charge of data processing, and/or the parties shall act as the persons responsible for co-processing.

#### **For the personal data processing, an authorized person:**

- shall process data only in accordance with a written task or instructions of the person in charge of processing, only for the purposes specified in a relevant contract;
- shall ensure that natural person(s) directly involved in data processing is(are) committed to maintaining confidentiality;
- shall ensure security of data in accordance with the statutory requirements, including, taking relevant technical and organizational measures for protection of information containing personal

data from accidental or illegal destruction, alteration, disclosure, acquisition, damage or any other form of unauthorized or illegal use and accidental or illegal loss;

- shall ensure that all actions performed in relation to the data available in electronic form (including incident-related information, data collection, modification, access thereto, disclosure (transfer), connection and deletion) be recorded (including the so-called logging) and a person responsible for the action could be identified; in case of data processing in non-electronic form, a person authorized to process it shall ensure the recording of all actions related to data disclosure and/or modification (including incident-related information);
- without a prior consent from the person in charge of data processing, shall not transfer personal data to a state and/or international organization that is not a member of the European Economic Area or is not included in the list of countries with relevant data protection guarantees provided for by a corresponding normative act of the Personal Data Protection Service / assignee thereof;
- shall provide relevant information to the person in charge of processing so as to ensure compliance with the commitments assumed under the Law of Georgia on Personal Data Protection and facilitate him/her in implementing the data processing monitoring;
- shall take appropriate organizational and technical measures so as to assist the person in charge of data processing in timely responding to the requests for personal data processing related information by the supervisory and other authorized body(ies), as well as in performing his/her obligation related to the implementation of the data subject's rights (data blocking, deletion, rectification, updating etc.) with due observance of the time-frame provided for by the Georgian legislation;
- It is inadmissible for the person authorized to data processing to transfer the data processing right to another person(s) without the consent from the person in charge of processing. In addition, if there is a transfer consent from the person in charge of data processing, the right to data processing shall be transferred by the person authorized to data processing on the basis of a written agreement, under which the data recipient (sub)contractor(s) shall take all necessary technical and organizational measures to protect personal data against accidental or illegal destruction, alteration, disclosure, acquisition, damage, or any other form of unauthorized or illegal use and accidental or illegal loss of personal data, and the all the obligations, the fulfillment of which under the present agreement and the Personal Data Protection Law are the responsibility of the person authorized to processing, shall apply thereto;
- shall, immediately or no later than within 24 hours, notify the person in charge of data processing in writing/ in electronic form about any unauthorized access to personal data or any other form of confidentiality violation (incident);
- in case of any data processing related dispute between the person in charge of data processing and the person authorized to processing, the person authorized to data processing shall immediately terminate the data processing and shall fully transfer all the available data to the person in charge of data processing;
- the person authorized to processing shall terminate data processing upon request of the person in charge of data processing, as well as in case of termination of the relevant agreement for any reason, and shall immediately or no later than within 10 (ten) calendar days (if the above-mentioned information is of substantial volume and/or needs to be searched for/accumulated) shall transfer personal data to the person in charge of data processing and shall delete/destroy without the possibility of further recovery the personal data transferred/shared to him/her and the

information/documentation containing this data stored in electronic or physical form, unless the data storage obligation is provided for by the legislation.

- for the sake of clarity, the parties hereby agree that the condition indicated in subparagraphs 'j-k' shall not apply to the personal data processed by the party enjoying a status of person in charge of data processing;
- the person authorized for processing shall compensate the person in charge of processing for the losses (including pecuniary sanctions imposed upon him/her), incurred as a result of violation of the requirements set forth in the present personal data policy and the applicable legislation by the authorized person;
- any issues related to the personal data processing shall be regulated by the person authorized for processing in accordance with the legislation of Georgia.

**Each person in charge of co-processing (hereinafter the 'co-processor'):**

- shall take corresponding technical and organizational measures to protect personal data from accidental or unlawful destruction, alteration, disclosure, access, damage, any other form of unauthorized or unlawful use and accidental or unlawful loss;
- shall allow access to information only to those employees, who perform the rights and duties provided for by the relevant contract signed between the parties and who are committed to observe the confidentiality of information, including upon termination of the official powers;
- shall closely cooperate with the co-processor so as to ensure compliance of data processing with the law;
- shall process data as part of the mutual cooperation, with due observance of the relevant contract and the legislation;
- shall cooperate and provide support to the co-processor within the scope of his/her competence in the implementation of data protection impact assessment, where the aforesaid is required by law or a relevant normative act;
- shall immediately or no later than within 24 hours notify the co-processor in writing/ in electronic form on any unauthorized access to personal data or any other form of confidentiality violation (incident). The notification should contain information about the circumstances, type and time of the incident; presumable categories and volume of data that were disclosed, damaged, deleted, destroyed, obtained, lost, altered without permission as a result of the incident, as well as the presumable categories and number of data subjects who were put at risk as a result of the incident; the person in charge of processing shall notify the co-processor about the measures implemented or planned by the person in charge of processing for the purpose of reducing or eliminating the alleged damage caused by the incident, as well as shall provide information about whether or not the person in charge of (co-)processing is going to notify the data subject about the incident and in what time frame;
- shall immediately notify the co-processor in writing/in electronic form on any request for disclosure of the processed personal data submitted by court, law-enforcement, regulatory/supervisory bodies and other agency;
- in case data are collected directly from the data subject, shall provide the latter with the information on the following: the purpose, grounds and time-frame of data processing; person(s) in charge of/authorized for co-processing, personal data protection officer (if any) etc., as well as the

data subject's rights provided for by the legislation (data blocking, deletion, rectification, updating etc.);

- shall ensure the data subject's access to the information on distribution of obligations and responsibilities among the persons in charge of co-processing; at the same time, the data subject's right to individually apply to any of the persons in charge of co-processing shall not be restricted;
- when accepting the data subject's application/ request/inquiry submitted for the purpose of implementation of his/her statutory rights (data blocking, deletion, rectification, updating etc.), the co-processor receiving the request shall nominate a co-processor in charge of review of the request and, within a reasonable time-frame, in a manner so as not to violate the review period set by the legislation, shall forward the aforesaid request for response. A co-processor initially accepting the application shall ensure all the necessary communication with the data subject;
  - a co-processor in charge of review of the request shall be determined as follows: if the data subject's data are part of the data set/ data aggregate that could be assigned to a single particular co-processor, the latter shall be in charge of review of the data subject's application. In other case, a co-processor who accepted the data subject's application (to whom the data subject has applied) shall be in charge of review of the application;
- persons in charge of data co-processing shall support and assist each other and shall facilitate implementation of the data subject's rights stipulated by the Law of Georgia on Personal Data Protection (data blocking, deletion, rectification, updating etc.), in the manner and within the time-frame prescribed by the legislation;
- shall implement all other actions foreseen by the legislation for the person in charge of co-processing;
- issues relating to the co-processing of personal data that are not provided for in the policy herein shall be regulated in accordance with the Georgian legislation.

## Clause 7

### Rights and obligations of data subject

#### **Rights of the data subject**

- Right to have access to information on data processing and to obtain a copy – a personal data subject shall be entitled to obtain information with regard to collection and use of his/her personal data. Namely, which particular personal data are processed, the purpose for which the personal data are processed and the grounds for data processing, data collection procedure, the period for which personal data are stored, the recipients of the personal data etc. In addition, a personal data subject is entitled to obtain the copies of the personal data that are processed;
- Right to rectify, update and fallout personal data – a personal data subject shall be entitled to request rectification, entry and/or updating of the personal data provided that the data processed by the company are invalid, incomplete or inaccurate and shall provide it with necessary information;
- Right to stop processing, erase or destroy data - a personal data subject shall be entitled to have his/her personal data erased, destroyed or no longer processed (including profiling, if available);

- Right to block personal data – a personal data subject shall be entitled to have his/her personal data blocked (restriction of processing), when the accuracy of the personal data is disputed by him/her or he/she requests termination of data processing, erasure or destruction of personal data for the period allowing to check the accuracy of the personal data and consider the request; when the matter concerns unlawful processing, the data subject shall refuse to delete the personal data and instead request blocking of the personal data; the Company no longer requires the personal data for processing purposes, but the data is needed to file a complaint/lawsuit; when there is a need to store data for the purpose of using them as evidence;
- Right to data portability - a personal data subject is entitled to receive the personal data that he/she has provided to a data processor in a structured, commonly used and machine-readable format or to request transfer of those data to another person in charge of data processing. The company is entitled to refuse to meet the data subject's request, provided that it is technically impossible and/or is related to unjustified expenses, time or other resources;
- Rights related to the automated individual decision-making – a personal data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling (if available), except for the cases, when the decision-making is based on profiling: a) is based on the data subject's explicit consent; b) is necessary for entering into or performance of a contract between the parties; c) is envisaged by law and/or subordinate legislation.
- Right to withdraw consent – a personal data subject is entitled to withdraw his/her consent at any time, provided that it is not at variance with the statutory requirements. The right to withdrawal can be implemented when the processing is based on the data subject's consent. Withdrawal of consent does not result in cancellation of legal implications arising before and as part of the withdrawal of consent. However, in case of withdrawal of consent, the company may not be able to provide the subject with a perfect product;
- Right to appeal – a personal data subject is entitled to appeal to the Personal Data Protection Service if/her believes that his/her personal data are processed in violation of the statutory requirements;

**Data subject shall:**

The data subject shall be responsible to ensure that the information provided to the Company is accurate and up-to-date. If the available information is invalid and/or incomplete, the data subject shall immediately notify the company thereof. If the data subject provides the company with the third-party related information (representative, contact person, etc.), including but not limited to their personal data, he/she shall obtain the consent of these persons for the transfer of their personal data to the company and its processing before transferring this information to the company, and in such a case , the company is released from responsibility. In addition, when providing personal data to the company, the data subject shall not apply the automated means that may pose risk to the company's safety and security.

**Note:**

The right to the protection of personal data is not an absolute right, which implies that interference with the area protected by this right is justified to achieve a legitimate goal, using necessary and proportionate means, when the interference does not imply a violation of the right. The above-mentioned right can be restricted if their realization poses risk to the following:

- national security, information security and cyber security and/or defense interests;
- public security interests;
- crime prevention, crime investigation, criminal prosecution, execution of justice;
- country's important financial or economic (including monetary, budgetary and tax), public health and social security interests;
- detection of violations of professional (including regulated profession) norms of ethics by the data subject and imposing responsibility upon him/her;
- the rights and freedoms of the data subject or other persons;
- protection of state, commercial, professional and other types of secrets stipulated by law;
- justification of the legal claim or counterclaim.

## **Clause 8**

### **Purpose and grounds for processing**

Personal data could be processed for different purposes and on different legal grounds, including:

#### **Purpose:**

- identification/verification of data subject and delivery of company products;
- access to data for the regulator or other supervisory/administrative body and audit companies in the cases stipulated by law and in a defined manner;
- preparation of various statements, studies and/or reports;
- provision of data security;
- prevention, detection and suppression of crime, property and security protection for the performance of the company's legal obligations;
- sending/delivery of relevant correspondence/notification;
- full and due performance of the company's contractual/pre-contractual obligations and/or monitoring of the subject's contractual/pre-contractual obligations;
  - marketing purpose, which implies that the company, with the data subject's consent, periodically offers various products, develops/plans/improves/implements marketing activities with due account for the data subject's feedback;
  - protection of the company's and/or third party(ies) interest and/or legitimate rights, disciplinary, administrative proceedings/judicial proceedings in court and other bodies, availability of legal claim/counterclaim;
  - planning and implementation of the company's corporate or other business processes, change in the company's entrepreneurial/corporate and organizational field.

#### **Grounds:**

- subject's voluntary consent to data processing;
- obligations stipulated by the legislation;
- necessity, prompted by conclusion of contract with the subject or performance of the available contract;
- consideration of proposals, statements, complaints, lawsuits or other types of claims;
- necessity, prompted by protection of the company's or third-party legitimate interests;
- legitimate interest in ensuring financial, legal, technical and other kind of the company's due, well-tuned, updated and improved activity;
- public access to data;
- crime prevention, detection, security and property protection, the purpose of protecting public order, as well as protection of classified information;

***Note:***

Special category data are processed with the data subject's written consent, whereas in the case of biometric data – data are processed if it is necessary for the implementation of activities, for the purpose of protecting person's property and security, as well as to prevent the disclosure of classified information;

The company is entitled to process the data for any other purpose as prescribed by law, as well as in case the post-processing purpose is compatible with the initial purpose

**Clause 9**

**Source of data acquisition**

Subject's personal data are collected by the company:

- directly from the data subject;
- from the third party(ies) – including, but not limited, to the following person(s):
- publicly accessible sources;
- subject's agent/legal representative, contact person;
- parties to a transaction/pre-contractual relations;
- governmental and non-governmental, civil, commercial, public institutions; local self-government and governmental bodies, local structures/bodies/agencies/LEPLs thereof; natural and legal persons, legal and non-legal (non-commercial) entities of public or private law, persons' associations and other bodies, stipulated by the legislation ;
- state tax bodies and other financial organizations;
- service providers - including, but not limited to, company's outside auditors, consultants, advisers, courier and/or research organizations, web tool and/or application providers, IT service providers, utility service providers and/or any other persons with similar functions.

**Clause 10**

## **Data transfer**

For the performance of the company's statutory obligations, protection of legitimate interests, as well as for full-fledged and due communicate with the subjects, their provision with relevant products, fulfillment of the obligations and exercise of the rights assumed under the contracts /pre-contractual relations, depending on the context and purposes of data processing, the company may transfer personal data, including but not limited to the following categories of third parties:

- subject's agent/legal representative, contact person;
- parties to a transaction;
- governmental and non-governmental, civil, commercial, public institutions; local self-government and governmental bodies, local structures/bodies/agencies/LEPLs thereof; natural and legal persons, legal and non-legal (non-commercial) entities of public or private law, persons' associations and other bodies, stipulated by the legislation;
- state tax bodies and other financial organizations;
- insurance companies;
- service providers - including, but not limited to, company's outside auditors, consultants, advisers, courier and/or research organizations, web tool and/or application providers, IT service providers, utility service providers and/or any other persons with similar functions.
- company group enterprises;
- other third parties, with the subject's consent.

## **International data transfer**

International data transfer can be carried out, where necessary. In this case, the company undertakes, to the extent possible, to ensure the safe and confidential transfer of data, in full compliance with the policy herein.

If the subject is located in the EU or EEA area and represents a data subject defined under the GDPR and the data is shared outside the EU and EEA, the data may be shared in different cases, for example:

- a country to which the information is shared enjoys relevant protection guarantees under the Georgian law and/or the European Commission's resolution;
- unless the law provides for relevant reservations, and/or there is a corresponding resolution of the European Commission, personal data may be transferred to a third country or an international organization only in the case, the company takes appropriate measures in accordance with the applicable legislation and/or GDPR. In addition, the subject can receive information about the relevant measures through the communication channels specified in this policy.
- unless otherwise provided for by a corresponding legislation, and/or in the absence of the European Commission's resolution or relevant guarantees, including Binding Corporate Rules approved by the European Commission, personal data can be transferred to a third country or international organization only in the following cases:
- if the data subject has explicitly consented to the data transfer, after being provided detailed information on the potential risks of the data transfer;

- if the data transfer is necessary for the performance of a contract between the data subject and the data processor, or for the implementation of pre-contractual measures taken upon the data subject's request;
- if the transfer is necessary for the conclusion or performance of a relevant contract, executed for the best interests of the data subject;
- if the transfer is necessary for important reasons of social/public interest;
- if the transfer is necessary for the exercise or defense of legal claims;
- if the transfer is necessary for protection of the vital interests of data subject or of other persons, where the data subject is incapable of giving consent.

***Note:***

In the event the subject refuses to transfer data to the third parties, including international data transfer, in the manner as prescribed by the legislation, this could possibly lead to a delay or impossibility of delivery of the relevant product/performance of obligations/exercise of rights etc.;

A third party receiving the relevant information shall ensure confidentiality of personal data and the company shall not be responsible for the violation of the confidentiality of the aforementioned information by a recipient of information, unless otherwise provided for by law. The company shall not be held liable for an unauthorized third-party access to personal data in course of provision of this data to the company (including the platforms used for remote provision).

**Clause 11**

**Video/audio monitoring**

Video monitoring of the external perimeter of the building(s) and audio monitoring of the company's incoming and outgoing calls is carried out in the company through the video surveillance system (CCTV) to ensure prevention, detection/investigation of crime, protection of public safety, personal and property security, protection of classified (confidential) information and performance of other important tasks within the scope of the company's legitimate interests (including incident management and protection of consumer rights, process monitoring, risk management, creation of legally valid evidence and, in the cases stipulated by legislation, their transfer to the relevant bodies for further examination, etc.).

Video surveillance is carried out in a round-the-clock mode, whereas the material is recorded in case a movement is detected in the surveillance perimeter, audio monitoring is carried out upon the need, in accordance with the measures introduced to promote the company's activities.

Corresponding warning signs with information on video surveillance are placed by the company in a visible place. As for the audio monitoring, a subject is informed by the company about the audio monitoring before recording the conversation or immediately upon starting the recording.

Some effective and adequate technical and organizational measures have been taken by the company to prevent unlawful/accidental disclosure, inappropriate use /dissemination of data displayed on recordings. In particular:

Physical security of the surveillance system has been ensured and they have been positioned in a secure room(s), where only the authorized personnel are allowed entry, with due account for their duties and their official need for access to records;

Appropriate measures have been taken for the information security of the system, in order to prevent unlawful access from the Internet and computer network;

Any action taken in relation to the data available in the surveillance systems is recorded;

## **Clause12**

### **Biometric data processing**

Where the remote connection is the only means of subject's communication with the company, in order to identify the subject and deliver the company's products to him/her remotely, as prescribed by the law, the subject shall go through an electronic identification process, which may imply identification of the subject through personal data, including biometric data. Biometric data are physical data (for example, a facial feature and expression) processed through technical means, allowing for unique identification or verification of subject's identity.

The remote identification process may involve taking a photo of the identity document and a dynamic selfie, comparing the aforesaid photo and the selfie, as well as checking the data of the produced document and the validity thereof.

Biometric data processing is important for ensuring security of the company's activity and prevention of disclosure of the confidential information, including data accuracy and validity check, which is important for verification of the subject's identity, prevention of any unlawful actions, as well as for ensuring full-fledged product delivery.

## **Clause 13**

### **Direct marketing, cookies**

#### **Direct marketing**

The company is entitled, in accordance with the company's data protection policy, to process, either independently or through the authorized and/or related person(s), the subject's personal data so as to individually and directly communicate to the data subject (direct marketing) its offers/provide information about the company's products, services, campaigns etc., by phone, mail, via e-mail, digital banking, mobile app(s) and/or through any other available telecommunication/electronic means.

The company's goal is to provide the subject with a choice regarding the use of his/her personal data for direct marketing and advertising purposes. In the absence of consent to the data processing for the purpose of direct marketing, the company will be deprived of the opportunity to offer customized services/products to the subject under the above-mentioned conditions.

Upon request to stop data processing for direct marketing purposes, only electronic communications of an advertising nature will be stopped. Communication with the subject using the contact data kept in the company will be maintained with regard to the issues arising as part of the company-subject relations;

If the advertising/informational messages are communicated directly through the company's service points (e.g. advertising banners, leaflets, verbal offers etc.), it shall not be regarded as direct marketing and the subject shall not be entitled to request that the aforesaid messages no longer be shared;

### **Cookies**

When using the company's web-site and other remote platforms, the so-called cookies (datasets) about the subject are collected for the security purposes, as well as with the aim to improve the company's products, personalize the subject, simplify navigation, offer information in a desired format, improve search parameters, secure user authorization, optimize marketing and web-page design and ensure better user adaptation

The following could be identified through cookies:

- operating system version;
- device model and other unique identifiers;
- duration of the user session on a web-site;
- information on the pages browsed;
- online navigation history;
- browser-related information;
- information on the actions taken on the company's web-site;
- geolocation from which the web-site was accessed;
- language that the subject selected to familiarize with the information.

When visiting the company's web-site and remote channels, the subject can accept /decline cookies and/or manage the purpose of using cookies upon his/her will, as well as to block or restrict the use of cookies on any web-site from the browser settings and the device used for the Internet access. In the same way, cookies that are already stored in the device can be deleted.

### **Clause 14**

#### **Security and storage period**

To fulfill the obligations set forth in the present data protection policy and relevant legislative and/or subordinate normative acts, with the aim to prevent unlawful access, processing, loss, destruction, disclosure and other unlawful actions, the company has obtained relevant technical and organizational guarantees, including:

- security of electronic equipment;
- security of tangible files;
- building security;
- available physical, electronic and regular control mechanisms;
- restricted access to personal data for the company's personnel or other individuals, within the scope of confidentiality, in accordance with their activity, assigned duties and tasks to be performed

Personal data shall be stored in the company for a period of 10 (ten) years from the date on which the relationship between the subject and the company ends, and where the aforesaid period is not suffice - for the period necessary to achieve the purposes for which the aforesaid data were collected, including any legal, regulatory, tax, accounting purposes or for the purpose of meeting the reporting-related requirements.

Records obtained through video/audio monitoring shall be stored for 1 month and/or for the period required for achieving a particular goal, upon which it shall be deleted by default, unless there is a need or legal grounds for data storage for a longer period of time.

#### **Amendments**

Any amendments to the personal data protection policy herein shall be published on the company's web-site.

**Date: 01.03.2024**