# Privacy Policy

## 1. Definitions

**1.1 We or Data Controller** – means Magticom Ltd (identification number: 204876606) that determines, alone or jointly with others, the purposes and means of data processing, and processes data directly or through the Data Processor.

**1.2 Data Processor** – means a legal entity or a public institution processing data for or on behalf of us.

**1.3 You** – means a natural person who uses, has intended or expressed interested to use any of our products or services, as well as the representatives and third persons who are related to you and whom you informed us or duly indicated to us about.

**1.4 Data processing** – means any operation performed in relation to data by us or by the Data Processor for or on behalf of us, whether with or without the use of information technologies, including collection, gathering, access to, audio surveillance, video surveillance, organization, storage, alteration, restoration, request for access to, sharing, use, blocking, erasure, or destruction of data.

## 2. Introduction

**2.1** We are orientated to protect your personal data and are keenly aware that the personal data that you entrust to us are, in light of their content and nature, valuable and important to you and, our primary responsibility is to protect them and ensure their privacy.

**2.2** In this Privacy Policy, we explain to you in detail what types of data we process, how we collect data about you, how data are processed when you use our services and buy products from us, on what basis and for what purposes we use your data and who we disclose such data to. We also explain your rights relating to data and the terms for exercising these rights.

**2.3** Aside from complying with the requirements of the data privacy legislation, we are committed to adhere to high ethical and moral standards when processing data, as we believe that the secrecy of communication and private life is one of the fundamental human rights and, therefore, it is our duty to protect your personal data and handle them with care.

## 3. Why and on what basis we collect your personal data

**3.1 You declared your intention or signed a contract with us to receive our services or buy our products**. In this case, the processing of your data is necessary to perform the obligations under the contract signed or to be signed with you. For instance, we need your data to manage your subscriber or your other electronic account, bill for the services, and provide our products and services to you.

**3.2 You declared your consent.** For instance, if you decided to take part in any survey, draw, campaign, contest organized by us or declared your consent to receive promotional information and news, offers and materials as part of direct marketing.

**3.3 We have the right to protect our legitimate interest,** to protect ourselves from wrongful, fraudulent acts, to protect our communications network, and demand that users perform their obligations. It is also our legitimate interest to develop and refine our services, diversify the offered products and activities. This implies the improving the current services and introducing new in-demand services, offering tailored services and products to you, developing the communications network, implementing new technologies aligned with your demands and individual style of using services, and collecting debts, if any.

**3.4** **Data processing is necessary to perform the obligations imposed on us under the legislation of Georgia.** For instance, in line with the requirements established by law, we are required to precisely identify you as a service recipient. We also need to monitor the services provided to you and the amount of such services in order to precisely calculate and bill the charges, remedy any defect in services, and perform to mandatory quality indicators and improve services. We are also required to retain the data and geolocation data generated in connection with electronic communications transmission and perform the obligation to record and request such information from public institutions.

**3.5** **Data processing is provided for by law.**

**3.6** For instance, we are required to retain the data and geolocation data generated in connection with electronic communications transmission and perform the obligation to record and request such information from public institutions.

## 4. Scope of application

**4.1** This Privacy Policy applies to any natural person (not legal entities) whose data are processed as part of our provision of services.

**4.2** Therefore, this Privacy Policy is aimed to inform the following categories of natural persons of the processing of their data:

**4.2.1** Our customers, whether fixed network or mobile network subscribers.

**4.2.2** Our future potential customers.

**4.2.3** Natural persons using our services or products (e.g., family members of our customers, corporate customer employees).

**4.2.4** Customers of any other electronic communications network operator who currently use our communications network.

**4.2.5** Representatives and contact persons of our corporate customers (e.g., corporate customer employees).

**4.2.6** Our former customers.

**4.2.7** Representatives and contact persons of our suppliers and partner companies providing us with services and products.

**4.2.8** Visitors to our subscriber service centers.

**4.2.9** Our website visitors and our mobile application users.

**4.2.10** Participants of draws, campaigns or contests organized by us.

**4.2.11** As our user, you may allow your family members, friends, guests or your employees to receive our services and products. For instance, this would happen when you allowed them to get connected to your Wi-Fi network that implies that we would process certain data about them and, therefore, this Privacy Policy encompasses such processing, too. In such case, it is important to consider that we have no opportunity to inform them. Therefore, we hope that as our user, you inform them thereon under your responsibility.

## 5. Types of data we process about you

**5.1** This clause informs what types (categories) of personal data we process about you and how these data are distributed by categories. You can see Clause 5 to see what categories of data are processed and Clause 8 to see what are the purposes and grounds of their processing.

### 5.1.1 Data collected from you (information that you provide to us)

**5.1.1.1** [In order for you] to use our services and products, we need to collect certain data about you. The data that we collect could be of different categories, depending on the circumstances, for which we need to collect them. For instance, we may collect such data as your first name and last name, address, citizenship, personal number, data of birth, sex, age, contact phone number and email address or your ID information allowing your identification.

**5.1.1.2** We may collect data about you by a variety of means, for instance, when you make a visit to our subscriber service center or sales office, when reading your ID as part of your remote identification process, including when signing up to our portal. Information is also collected when you buy any product or service from us (including when placing an order or making a purchase of products or services through a website or our portal, via telephone communications, by way of an onsite or offsite transaction, we may also collect data verbally, at customer service centers and sales offices, during a phone call to the subscriber service hotline, by email or tangible correspondence, electronic order at our portal or during communication with us via social media.

**5.1.1.3** From the moment you become our customer, we collect the following categories of data about you:

- **Identification and contact data:** this is the information, by which you are identified and by which communication with you is carried out (first name and last name, address, contact (mobile) phone number, email address, password, if any, VAT payer identification number, name registered at our portal an any other identifier, etc.), citizenship, personal number, date of birth, sex, age, your ID information and the photo on your ID and, in addition, a specially taken photo and/or visual image, including a motion video image.
- **Personal number:** personal 11-digit number or document number indicated in your identification document or passport.
- **Corporate data:** information on the company that you represent or are an employee of.
- **Personal aspects:** any information relating to your specific characteristics/features such as age, sex, date of birth, place of birth, citizenship, etc.).
- **Financial data:** any information relating to your bank details as a user such as data on your credit or debit card as well as information on your bank account number and 16-digit bank card number or any other bank details.
- **Data on customer activities:** such information as any record of your, as a user's, communication with us, any visit to our portal, website or subscriber service center, activated or purchased services and products, including the identifiers assigned on or within the scope of our portal.
- **Survey-related information**: any information relating to the questions asked by us and answers given by you as part of any survey organized by us, such as our service quality, satisfaction, and demands.

**5.1.2** Collected information (information that we may collect from the third persons)

**5.1.2.1** In some cases, we may collect information from the third persons certain data about you such as **identification and contact details** and **personal aspects**.

**5.1.3** Generated data (the information that we receive as part of your use of our products and services)

**5.1.3.1** We collect the information relating to your use of our products and services and your visits to our website or subscriber service centers or your communications to our subscriber service holtline.

**5.1.3.2** **Subscriber service department or hotline audio surveillance and other activity records**: audio and textual records of the communications carried out via an audio surveillance system to our subscriber service department or hotline by you as a user (audio recording and electronic correspondence to the subscriber service hotline via the audio surveillance system).

**5.1.3.3** **Photo and video records:** any photo and video footage captured by any video surveillance camera mounted at our subscriber service centers and processed for security purposes.

**5.1.3.4** **Internal identifiers:** the records that we use on you as a user (user number - UID and information on your electronic account);

5.1.3.5 **Technical identifiers:** any identifiers used for technical purposes and and related to a user's specific detail such as a mobile equipment identifier (IMEI number), service ID, international mobile subscriber identity (IMSI), handset electronic serial number (ESN), IP address, ticket ID, case ID ….

5.1.3.6 **Subscriber product and service data:** information on the products and services a user has signed up for or subscribed to (descriptions and list of the devices placed with you to use our services or products).

5.1.3.7 **Product and service use data:** any information relating to the use of our products and services by you as a user (as part of the mobile communications services, use of the data transmission service, use of the voice call service, use of our applications, etc.). This also includes any information on the date and time of their use, duration of their use, the location of their use, charges billed to you and the time of payments made by you, as well as any information on the service related user account, including outstanding charges, completing the user account with information on services activated and deactivated on it, and the points granted and activities performed on the user account.

5.1.3.8 **Equipment data:** any information on the equipment that you use (equipment (decoder, modem, router) type, brand, software) or on the equipment (type, brand and handset IMEI) that is connected to the Wi-Fi network and/or the mobile communications network.

5.1.3.9 **Billing information:** any information relating to billing data (payments, outstanding amounts, invoices).

5.1.3.10 **Data generated as part of electronic communications transmission:** any information collected during the user's use of a mobile or fixed communications network (detailed information on any electronic communication - electronic communication identification data, IPTV logos, user's handset IMEI number, location where the communication or internet is provided.

5.1.3.11 **Geolocation data:** your handset location collected and recorded with your use of our mobile communications network. The information includes [data] on your approximate location that we need in order for you to be able to make, send, receive or use calls, SMS or over-the-top se(OTT) services from and at a specific communications network location. This is referred to as the location identified by the communications network that is determined by the communications service antennae mounted nearest at any specific time the service is received, without determining your exact location. This is different from the geolocation determined by GPS using man-made satellites that is more precise, which is used by your handset controlled directly by you, unbeknownst to us, and which you can put on or off at any time from your handset.

5.1.3.12 **Usage patterns (styles of use):** any information relating to your ordinary style of use of our products and services such as history of purchased products and services, IPTV watch pattern, website visitor behavioral pattern;

5.1.3.13 **IPTV user behavior:** the data generated in connection with the user's use of our IPTV.

5.1.3.14 **Biometric signature data:** the information electronically generated/saved as a result of the user's electronic signature made on the electronic signature board in our possession that includes signature behavioral patterns (force of application, acceleration, and other parameters), with the signature being related to the contents of the information (subject-matter of contract/transaction) displayed on electronic signature board at the moment of signature.

5.1.4 Produced information (information that we produce from collected or generated data)

5.1.4.1 In certain cases, we use collected, processed and generated data to make certain inferences.

5.1.4.2 **Profiling information:** any information used to distribute customers to different segments or groups user patterns, frequently visited locations, preferences, personal interests, products and services signed up (subscribed) to, poor payer).

5.1.5 How long we retain/process data about you

**5.1.5.1** The retention period for the personal data we process depends on the purpose, for which such data are processed. See Clause 8 for information on such periods.

## 6. How we collect data about you

**6.1** Mostly, we collect data about you when:

**6.1.1** You intended or sign up as a user to receive our products and services or participate in any contest, survey or draw organized by us, or register in any case a user account or any other electronic account with us.

**6.1.2** You buy any product or service from us, inter alia, you buy products or services from our website online, with our portal, by telephone communications, in our subscriber service center, including by way of a remote transaction, in any other sales office or in any other form used by us.

**6.1.3** You call our subscriber service center or apply to us with any question or complaint.

**6.1.4** You perform a subscription to any of our services (sign up for such service).

**6.1.5** You perform any activity, changes, activation/deactivation of any of our services on your user account.

**6.1.6** You use our communications network to receive mobile as well as fixed Internet, including with the use of a WiFi network.

**6.2** Where appropriate, we can also collect information about you from other sources, including but not limited to such organizations and companies as fraud prevention agencies, business manuals and credit information organizations. We can also collect information about you as part of our other activities as well as from partner companies and other companies.

## 7. How data will be shared with the third persons

**7.1** We share your personal data with different categories of our subcontractors, suppliers, partners, contractors, persons responsible for co-processing, public institutions, and other third persons. When you use any of our products or services, we share data with the third persons taking part, cooperating or involved jointly with us in the creation of such product or service. We share personal data with public institutions when we are required to do so by law. In certain cases, data sharing is based on your explicit consent or when we think it to be an adequate and relevant measure in our legitimate interests. Paragraph 7.2 below sets forth categories of the third persons we share data with.

**7.2** Contractors, suppliers and other third persons:

- Other electronic communications network operators and service providers;
- IT service providers;
- Communications and network equipment suppliers;
- Payment service providers;
- Billing service providers;
- Digital content providers in the service sector;
- Communications software suppliers;
- Marketing research agencies;
- Direct marketing service providers;
- Companies operating in the debt collection sector;
- Law firms.

**7.3** We may share data with companies located beyond borders if the country in question has adequate privacy guarantees under the applicable laws.

**7.4** Data may be shared with public institutions to ensure compliance with the legal requirements established by the applicable laws.

**7.5** Notwithstanding the persons in Article 8 with whom data are shared, according to the requirements of the applicable laws, to the extent of the legal requirement, data may be shared with:

- Judicial bodies;
- Law-enforcement, counterintelligence, national security services;
- Personal Data Protection Office;
- Tax authorities;
- Competition Agency;
- National Communications Commission.

## 8. For what purposes (other than marketing purposes) we process your data

**8.1** This article defines the purposes (other than marketing and product and service sales purposes), for which we process personal data. The purposes are provided by different categories. Each purpose is identified in a short section that contains such important information as the type of data the purpose applies to, the legal basis for processing such data, the period of processing/retention of such data, the categories of third persons the data are shared with if reasonable and legitimate, and the procedure for a data subject to exercise his/her rights where such rights differ from the general rights that the data subject has, as set forth in Article 9 below.

### 8.1.1 Security purposes

#### 8.1.1.1 Video surveillance

**What types of data do we use?**
**Processed and generated data:** photo and video footage.

**What is the processing based on?**
Our legitimate interest (Article 5(1)(a) of the Law on Personal Data Protection) – ensuring the security of our users, visitors, employees and assets; and

Data processing is envisaged by law (Article 5(1)(c) of the Law on Personal Data Protection), we have the duty to mount automatic photo and/or video surveillance equipment on some of our buildings and structures – at subscriber service offices.

**For what period do we process data for such purpose?**
The photo and video footage of our video surveillance cameras are retained for a period of 6 (six) months, subject to the requirements of the relevant laws, except where such footage contains evidence of any crime or harm or is capable of identifying any victim, witness or accused.

**Who are these data shared with?**
The photo and video footage of our video surveillance cameras may be shared with law-enforcement authorities, to comply with a legal obligation, subject to a legal requirement.

**How can you access the data?**

If you wish to request access to video surveillance footage, provided you have identified cameras, you must indicate the date, location and the time period the video surveillance cameras recorded the data, and you can email such request to the Personal Data Protection Officer (provided on our website). However, please note that if the time period or photo or video footage requested by you contains data on any identifiable third persons, we'll deny your request for access to such data to ensure the protection of the rights and security of potential data subjects. Please see Article 9 for more information on the exercise of your rights as a data subject.

There are video surveillance cameras mounted around our subscriber service centers and other buildings, and the surveillance warning sign (icon) is put up conspicuously at the entrance to such building. The video surveillance system is used in accordance with the relevant legal requirements to prevent, detect and discover crimes against persons or property.

#### 8.1.1.2 Visitor management

**What types of data do we use?**
**Data collected from you: identification data** and contact details

**What is the processing based on?**
Our legitimate interest (Article 5(1)(a) of the Law on Personal Data Protection) – ensuring the security of our administrative office.

**For what period do we process data for such purpose?**
We retain such data for a period of 6 (six) years after a visitor has actually made a visit to our office.

**Who are these data shared with?**
The data may be shared with the partner company ensuring the administration and maintenance of the visitor/guest management system.

A visitor badge/pass permit bearing a number will be issued to you upon your scheduled visit to our administrative office and your data will be recorded in the administrative office reception.

### 8.1.2 Audio surveillance data for quality control purposes

**What types of data do we use?**
**Data collected from you: identification data** and contact details
**Generated data:** Subscriber service department and hotline audio surveillance and other activity records.

**What is the processing based on?**
Our legitimate interest (Article 5(1)(a) of the Law on Personal Data Protection) – exercising control over and improve the quality of our subscriber service department operations.

**For what period do we process data for such purpose?**
We retain audio surveillance records for a period of 3 years from the occurrence of communication.

**Who are these data shared with?**

We do not share such data except as legally required under the relevant laws.

**How can you decline?**
You can decline directly with your action, namely, by discontinuing the communication at the time of the warning text.
Please see Article 9 for more information on the exercise of your rights as a data subject.

The reason why such data are processed in certain cases is to provide you as a subscriber with the information support generally provide to electronic communications users, assistance, including technical assistance regarding products and services. Therefore, these need are needed for us to provide you with information services as well as to help improve the services that we provide to our users.

### 8.1.3 When you intend to become a customer (contracting purposes)

**What types of data do we use?**
**Data collected from you: identification data** and contact details, personal number, personal aspects, financial data, user activity data.
**Generated data:** internal identifiers, technical identifiers.

**What is the processing based on?**
The necessity to process the data to perform our obligations under a contract with the data subject or to sign a contract at the request of the data subject (Article 5(1)(b) of the Law on Personal Data Protection) and the need to process the data to perform the obligations under the electronic communications legislation (Article 5(1)(d) of the Law on Personal Data Protection), namely our obligation to precisely identify the user.

**For what period do we process data for such purpose?**
We retain the data processed for such purpose for the period you are our user plus 4 years after the termination of the contract with us. If the contract is no longer signed, the data will be retained for a period of 1 year after they have been received (initially processed).

**Who are these data shared with?**
The data processed for this purpose may be shared with our partner companies involved in the provision of products and services to you, the electronic communications service providers you port out to, and to comply with any legal request as part any legal compliance.

Subject to legal requirements, before you become our user, we are required to process the data collected from you as well as the data generated by us (e.g., assigning a registration number, contact phone number or internal identifier to you) that we need to evaluate the availability of, provide and sign a relevant contract for the particular products and services requested by you. To provide fixed Internet services or IPTV services, we need to process your data in order to evaluate in advance whether it is technically possible to provide you with the requested service in the indicated location (geographical area).

### 8.1.4 When you are out customer

#### 8.1.4.1 Provision of our products and services

**What types of data do we use?**
**Data collected from you: identification data** and contact details, personal number.
**Generated data:** product and service user data, product and service usage data, technical identifiers, data generated upon transmission of electronic communications, and network location data.

**What is the processing based on?**
The necessity to process the data to perform our obligations under a contract with the data subject or to sign a contract at the request of the data subject (Article 5(1)(b) of the Law on Personal Data Protection) and the need to process the data to perform the obligations under the electronic communications legislation (Article 5(1)(d) of the Law on Personal Data Protection), namely our obligation to precisely identify the user.

**For what period do we process data for such purpose?**
We process the data for such purpose for the period you are you are our user plus 4 years after the termination of the contract with us.

**Who are these data shared with?**
The data processed for this purpose may be shared with our partner companies involved in the provision of products and services to you and in the and technical support for the process, the electronic communications service providers you port out to, and to comply with any legal request as part any legal compliance.

We need to process such data in order to provide you with the services you have requested, inter alia, when you use the voice call or SMS services, including in the fixed communications network, we need to process the data in order to ensure a reliable communication between the electronic communications initiator and the user called, and to properly switch telephone, data transmission and SMS traffic in our communications network.

Important information: **when providing services to you, we have no access to the content of the electronic communications. We process only the necessary information that ensures the functioning of our services and a proper transmission of electronic communications (e.g., the delivery of SMS to the relevant recipient), at which time our communications network is just a canal transmitting the communications content. Access to any communications content is strictly regulated and permitted only in the specific cases exhaustively listed in the Law of Georgia on Electronic Communications (Article 8).**

### 8.1.4.2 Interconnection with other electronic communications operators (provision of electronic communications services)

**What types of data do we use?**
**Generated data:** data generated upon transmission of electronic communications.

**What is the processing based on?**
The necessity to process the data to perform our obligations under a contract with the data subject or to sign a contract at the request of the data subject (Article 5(1)(b) of the Law on Personal Data Protection)

and the need to process the data to perform the obligations under the electronic communications legislation (Article 5(1)(d) of the Law on Personal Data Protection), namely our obligation to process and exchange data in accordance with the Georgian electronic communications legislation.

**For what period do we process data for such purpose?**
We process data for such purpose for a period of 4 years after the occurrence of communication.

**Who are these data shared with?**
We need to exchange (receive and transmit) the data with the other electronic communications operators involved in the implementation of the particular electronic communication, to ensure interconnection (physical and logical connection of electronic communications networks) while providing electronic communications services.

Interconnection is a key requirement in the process of any electronic communications services. To put it simply, interconnection enables you as our user to connect to any other operator's network, use data transmission services or reach others (whether by voice call or SMS) connected to such other operator's network, including in foreign countries, or use the services of any other communications operator.

Every electronic communications operator has a legal requirement to ensure access to its own electronic communications network and sign interconnection agreements with other communications network operators. As part of such interconnection, user data are exchanged to switch electronic communications, and for billing, comparison and billing purposes.

#### 8.1.4.3 Billing and accounting

**What types of data do we use?**
**Data collected from you: identification data** and contact details, personal number, financial data and personal aspects.
**Generated data:** internal identifiers, technical identifiers, product and service user data, product and service usage data, billing information და data generated upon transmission of electronic communications.

**What is the processing based on?**
The necessity to process the data to perform our obligations under a contract with the data subject or to sign a contract at the request of the data subject (Article 5(1)(b) of the Law on Personal Data Protection), our legitimate interest (Article 5(1)(a) of the Law on Personal Data Protection) and the Tax Code of Georgia. We need to process the data for billing, financial reporting, and issuing invoices to corporate users.

**For what period do we process data for such purpose?**
We process data for such purpose for a period of 4 years after the last specific payment or action.

**Who are these data shared with?**
Data for such purpose may be shared with those providing products and services on our behalf, those providing billing services to us. Besides, certain data may be shared with the companies that are your

employers or pay, within a different legal relationship with you, for the services we provide to you, also if you pay for our services through payment service provider channels, some of your data may be shared with such service providers or banks in order to complete such transactions.

Billing is related to nearly all the products and services we offer you. For that purpose, we use the data relating to your contract with us and your use of our products and services to calculate and invoice the fees due that also entails calculation of any relevant taxes. We also use your contact data to provide you with billing information and invoices. For instance, if you use payment service provider channels to you pay for our products or services, we will exchange your billing information, as further defined in paragraph 8.1.4.5 on third party billing.

#### 8.1.4.4 Collection process

**What types of data do we use?**
**Data collected from you: identification data** and contact details, personal number, financial data and personal aspects, user activity data.
**Generated data:** internal identifiers, product and service user data, product and service usage data, billing information.

**What is the processing based on?**
The necessity to process the data to perform our obligations under a contract with the data subject (Article 5(1)(b) of the Law on Personal Data Protection).

**For what period do we process data for such purpose?**
We process data for such purpose, including for financial and tax reporting purposes, for the period you are our user plus 4 years after the termination of the contract with us.

**Who are these data shared with?**
The data may be shared for such purpose with debt collection companies, the National Enforcement Bureau, and private enforcement agents.

If users delay paying any fees due, we have to take steps to collect such outstanding funds. In such case, to collect outstanding funds, we may process data to perform a variety of actions, namely:

- Classify such users (natural persons or legal entities, reasons for delay in payment or for non-payment) in order to plan appropriate subsequent steps.
- Giving users a notice of any respective outstanding funds.
- Restricting access to our services (telephony, IPTV and Internet) for such users.
- Classifying such users as bad users in our database.
- Applying to debt collection companies, the National Enforcement Bureau,

#### 8.1.4.5 Third party billing

**What types of data do we use?**
**Data collected from you: identification data** and contact details, financial data.

**Data obtained from third persons: identification data** and contact details.
**Generated data:** internal identifiers, technical identifiers, product and service usage data, billing information.

**What is the processing based on?**
Our legitimate interest (Article 5(1)(a) of the Law on Personal Data Protection) to offer our users safe third party billing.

**For what period do we process data for such purpose?**
We process data for such purpose, including for financial and tax reporting purposes, for a period of 4 years after the performance of a particular payment transaction.

**Who are these data shared with?**
The data that includes the user number only may be shared with the third party service providers, e.g., e-commerce merchants.

**How can you decline?**
You can decline directly with your action, namely, by not accepting our offers for the purpose of third party products or services.

We offer our users the opportunity to directly pay for third party (another company/merchant) products or services. For instance, when you intend to buy any third party service, the service could be related to our service and for convenience we'd supply the payment received from you to such third persons.

### 8.1.5 Remote identification/verification process

**What types of data do we use?**
**Data collected from you: identification data** and contact details.
**Data obtained from third persons: identification data** and contact details.

**What is the processing based on?**
The necessity to process the data in order to perform our obligations under the electronic communications legislation (Article 5(1)(d) of the Law on Personal Data Protection), namely, our obligation to to precisely identify users, and our legitimate interest (Article 5(1)(a) of the Law on Personal Data Protection) to identify/verify persons, when entering remote contracts, to prevent fraud, including by using the identification/verification services of third parties.

**For what period do we process data for such purpose?**
We process the data for such purpose for the period you are our user plus 4 years after the termination of the contract with us.

**Who are these data shared with?**
These data are shared in the process of identification/verification with the identification/verification service provider that in this case is the data processor.

**How can you decline?**
You can decline directly with your action when you decline to enter a remote transaction.

Under the Law on Electronic Communications, we are required to precisely identify users inasmuch as where any remote transaction is entered (the transaction is entered without a concurrent physical presence of the user and us), it is pertinent to identify users using a remote communications facility, in which case we may use the identification/verification services of third persons.

### 8.1.6 Electronic signature process

**What types of data do we use?**
**Data collected from you: identification data** and contact details.
**Generated data:** internal identifiers, technical identifiers, biometric data.

**What is the processing based on?**
The necessity to process the data in order to perform our obligations under the electronic communications legislation (Article 5(1)(d) of the Law on Personal Data Protection), namely, our obligation to to precisely identify users, and our legitimate interest (Article 5(1)(a) of the Law on Personal Data Protection) to identify and use a mechanism evidencing the user consent by means of an electronic signature in accordance with the legislation on electronic communications, electronic document and reliable electronic services.

**For what period do we process data for such purpose?**
We process the data for such purpose for the period you are our user plus 4 years after the termination of the contract with us.

**Who are these data shared with?**

Biometric data generated in the course of entering an electronic transaction are shared with a developed e-signature service provider that ensures electronic signature generation and data encryption as well as with LEPL Public Service Development Agency that issues appropriate e-signature certificates. If it becomes necessary to perform a forensic examination of signatures, the data may also be provided to the forensic bureau.

**How can you decline?**
You can decline with your direct action when you decline to enter our service contract electronically (using an electronic document), in which case you can enter the contract with us in a tangible form.

Processing the biometric data of your signature means generating an electronic document created after the data subject's e-signature through the e-signature cryptographic key certificate issued by LEPL Public Service Development Agency that maintains, in an unchanged form, the text appearing on the signature board at the moment the user signs and the encrypted biometric data of the signature. The biometric data becomes an integral part of the electronic document. The closed cryptographic key designed to de-encrypt the biometric data of the signature is not accessible to the company and the e-signature service provider, as only LEPL Public Service Development Agency has it. If necessary, e.g., when the user contests the

genuineness of a signature made by him/her, such data are de-encrypted only in order to conduct a forensic examination, by the authorized forensic bureau, so that neither the e-signature service provider nor we has any access to such data. The purpose of processing the biometric data of a signature is to identify the signatory to a contract when entering it between any user and us, enter the contract electronically, and simplify the process.

Important information: **when creating an electronic document generated during any electronic signature, we have no access to the e-signature biometric data. The e-signature service provider and we process only the necessary information that ensures the e-signature generation and the electronic document management system as well as the transmission/exchange of such data, at which time our communications network and the e-signature service provider platform are just a canal transmitting the communications content. If necessary, only the relevant authorized forensic bureau has access to such data through LEPL Public Service Development Agency.**

### 8.1.7 Dispute resolution/management

**What types of data do we use?**

The data types we may use to resolve/manage disputes depend on the matter at dispute and the content of each particular dispute. Normally, we process only the information that is necessary to identify you. **Data collected from you: identification data** and contact details, personal number). Depending on the content of a dispute, other data (such as: **data collected from you:** user activity data, also **generated data:** subscriber service department or hotline audio surveillance and other activity records, billing information, product and service user data, product and service usage data, biometric data of a signature, etc.)

**What is the processing based on?**

The necessity to process the data in order to perform our obligations under the electronic communications legislation (Article 5(1)(d) of the Law on Personal Data Protection) if the dispute involves our user, or our legitimate interest (Article 5(1)(a) of the Law on Personal Data Protection) to regulate a dispute where the dispute involves another person not being our user.

**For what period do we process data for such purpose?**

We process the data for such purpose for the period you are our user plus 3 years after the termination of the contract with us or, in other cases, for a period of limitation of contractual claims, after the end of a dispute.

**Who are these data shared with?**

The circle of the persons with whom the data could be shared depends on the matter at dispute and the content of each particular dispute (e.g., the data could be shared with law firms, private enforcement agents engaged by us in the regulation of the dispute).

As part of such dispute resolution, we will primarily process the data that are relating to your electronic user account in order to identify you, after which we may process such data as your payments, use of out products and services (e.g., billing information, payments, your product and service usage data).

### 8.1.8 Market research

**What types of data do we use?**

**Data collected from you: identification data** and contact details, personal aspects, research related information.

**Generated data:** product and service user data, product and service usage data, equipment data, billing information.

**Collected data: identification data** and contact details.

**Produced data:** Profiling information.

**What is the processing based on?**

Our legitimate interest (Article 5(1)(a) of the Law on Personal Data Protection) offer to users to take part in a market research.

Processing data as part of the market survey: your consent (Article 5(1)(a) of the Law on Personal Data Protection) to take part in the market research.

**For what period do we process data for such purpose?**

**Data collected from you: identification data** and contact details, personal aspects, research related information will be retained with you for a period of 2 years after the contract termination.

Other personal data, including those collected as part of a market research, will be retained for a period of 3 years after the end of the market research.

**Who are these data shared with?**

We obtain market research related data and share them with a variety of companies conducting such research.

**How can you decline?**

If you don't wish to receive future market research related offers, you can withdraw your consent by applying to us.

Please see Article 9 for more information on the exercise of your rights as a data subject.

We conduct market research to know your position on and improve our current and new products and services in order to:

- Evaluate the brand image and communication;
- Be aware of user needs and and behavior;
- Market and benchmark our products and services;
- Understand user satisfaction and loyalty.

### 8.1.9 Legal compliance

#### 8.1.9.1 Legal compliance regarding the retention of data generated upon transmission of electronic communications

**What types of data do we use?**

**Generated data:** data generated upon transmission of electronic communications, namely – electronic communication identifiers.

**What is the processing based on?**
The processing of such data is provided for by law (Article 5(1)(c) of the Law on Personal Data Protection), namely our obligation to process such data in accordance with the Law on Personal Data Protection (Article 8[5])

**For what period do we process data for such purpose?**
Retention periods for data generated upon transmission of electronic communications, namely electronic communication identifiers.

**User identity, contact details, information on the location of the mounted communications equipment, the user number assigned for the purpose of service provision, and any other details indicated in the service contract with the user** – are retained during the effective period of the electronic communications service contract and 4 years after its termination.

**Data needed to identify the communication equipment or possible equipment of the user, data needed to trace and identify the source of communication, data needed to identify the addressee of communication, data needed to identify the date, time and duration of communication, data needed to identify the type of communication, data needed to identify the location of the mobile communication equipment** – are retained for a period of 4 years after the occurrence of the communication concerned.

**Data on the account and payments (including service fees)** - are retained for a period of 4 years after the occurrence of the communication concerned.

**Who are these data shared with?**
The data are processed for such purpose within our company and may be shared, to the extent of the relevant legal obligation, with:

- Courts;
- National Communications Commission;
- Personal Data Protection Office;
- Competition Agency;
- Law-enforcement authorities, and
- Other authorities and agencies, in accordance with the requirements of the applicable laws of Georgia.

The laws of Georgia, including the Law on Electronic Communications, provides an exhaustive list of the data generated in connection with electronic communications that must be recorded and retained, the persons such data may be provided to and the basis for such provision.

#### 8.1.9.2 Geolocation data sharing

**What types of data do we use?**
**Data collected from you: identification data** and contact details.
**Generated data:** geolocation data (collected/recorded upon your use of our mobile communications network)

**What is the processing based on?**
The processing of such data is provided for by law (Article 5(1)(c) of the Law on Personal Data Protection), namely our obligation to process such data in accordance with the Law on Personal Data Protection (Article 8[4])

**For what period do we process data for such purpose?**
We do not retain geolocation data – such data are shared only in real time.

**Who are these data shared with?**
The data are processed for such purpose within our company and may be shared with:

- Public Safety Command Center 112
- Law-enforcement authorities, and
- Other authorities and agencies, in accordance with the requirements of the applicable laws of Georgia.

We are required to share with Public Safety Command Center, when they receive a report, your identification data and contact details and geolocation data that establish, in real time, automatic mode and as accurately as possible, the information on the geolocation of the initiating mobile communications equipment.

### 8.1.10 Data processing for marketing purposes

**What types of data do we use?**
**Data collected from you: identification data** and contact details;
**Generated data:** data generated upon transmission of electronic communications;
**Produced data:** profiling information.

**What is the processing based on?**
Your consent (Article 5(1)(a) of the Law on Personal Data Protection) to process data for direct marketing purposes and receive from us as well as from our contractors promotional SMS, emails, and voice phone calls. You may elect to give such consent at the time you enter a contract or at any time thereafter.

Your can give your consent in a differentiated manner by agreeing to receive information on products and services from us only or to receive notifications/offers from us as well as from our partner companies/contractors.

Promotional information from our partner companies/contractors means information from various companies regarding their products/services (e.g., campaigns and offers from insurance companies, equipment/household appliance stores, drugstores, etc.).

**For what period do we process data for such purpose?**
We'll process such data until you withdraw the consent you have given.

**How can I withdraw my consent?**

You may withdraw your consent to process your data for direct marketing purposes at any time by any of the methods provided on the website. We'll stop processing your data for direct marketing purposes within no later than 7 business days following your request. Consent may be withdrawn in a differentiated manner (e.g., refuse to receive messages from partner companies/contractors or completely refuse to receive messages from us as well as from partner companies/contractors).

Our stopping the processing of your data for direct marketing purposes does not mean that we will block messages (SMS) generated from any other communications operator's network or sent by any particular person at his/her responsibility for direct marketing purposes. You need to block such messages in the manner indicated in a particular message.

Withdrawal of consent does not apply to the receipt of messages that are informative or transactional in nature, such as the messages we may send to top up your user account balance, to inform you of service restrictions, bank messages of transfers, etc.

**Who are these data shared with?**
The data are processed for such purpose within our company and may be shared with:

- Advertising agencies;
- Advertisement clients;
- Various companies engaged in the retail or wholesale trade in different products and services.

## 9. What are my personal data protection rights and how should I exercise them?

**9.1** You have the rights defined by the applicable legislation of Georgia regarding the data that we process about you, namely, the right to:

**9.1.1** Request a detailed list of the data we process about you as well as the information pertaining thereto such as the grounds for and purposes of processing, retention periods, etc. (in this connection, a general list of the types of data, whether collected from you or from the third persons, processed, generated and produced by us, grounds for and purposes of processing, sources of data collection/obtaining, retention periods and/or criteria for their determination, your rights, legal grounds for and purposes of data sharing, and categories of data recipients are provided in Article 8 of this document).

**Despite the above, proactively published information, you may receive the information described above within no later than 10 business days following your request. In special cases, if there are compelling reasons to do so, this period may be extended by maximum 10 business days, with a prompt notice to you to that effect.**

**9.1.2** **Have access to the data that we process about you and have copies of such data** after you have paid the relevant fee charged by us (by printing information in a tangible form or recording information on any other data carrier electronically); you may have access to your data and/or receive their copies in the form that they are retained with us. If you so elect, you have the right to request copies of data about you in a different form if technically possible, in which case we may charge an additional reasonable fee.

**You have the right to have access to and/or have copies of the data described in the above paragraph within no later than 10 business days following your request. In special cases, if there are compelling**

**reasons to do so, this period may be extended by maximum 10 business days, with a prompt notice to you to that effect.**

**9.1.3** Request the **correction, updating and completion of your data** (if you find out that some of your data are wrong, inaccurate or incomplete). If we find out such instances independently from you, we'll correct, update and complete such data on our initiative, without your involvement and give you a notice to that effect except where the correction, updating and completion of data is related to the correction or elimination of a technical error.

**We'll ensure the correction, updating and/or completion of your data or give you a notice of the grounds for denying your request, by indicating the procedure to appeal such denial, within no later than 10 business days after you have filed your request.**

**If we find out, independently from you, that the data at our disposal are wrong, inaccurate and/or incomplete, we'll correct, update and/or complete such data as soon as reasonably practicable, and give you a notice to that effect within 10 business days following such correction, updating and/or completion. We have no obligation to notify you where the correction, updating and/or completion of data is related to the correction or elimination of a technical error.**

**9.1.4** Request that we **stop processing, delete or erase your data**. This right applies to the processing of your data that we carry out only by your consent (e.g., data processing for direct marketing purposes). In any case, if the data processing is stopped, it will apply only to a future processing of data, not the data that have already been processed – such processed data will be retained for the period defined by this Policy and the applicable laws. Further, we may refuse to grant such request if:

- There is some basis other than your consent under the applicable laws to process your data.
- The data are processed to comply with any legal requirement or substantiate a defense.

If we refuse for any of the reasons above, we'll substantiate such refusal.

**We'll stop processing, delete or erase your data, as per your request, within no later than 10 business days after you have filed such request and, as soon as we finish such actions, give you a notice of the performance of or refusal to perform the respective action within the same period of time, by indicating the procedure to appeal the refusal.**

**9.1.5** Request that we **block data** which means that we temporarily suspend data processing by your request and only retain such data. You have the right to request the blocking of data if there is one of the following circumstances:

- You contest the validity or accuracy of data;
- Data processing is illegal but you object to their deletion and demand their blocking;
- The data are no longer necessary to accomplish the purpose of their processing but you need them to file a complaint/claim;
- Your request is for termination of the processing of data, for deletion or erasure of data and the request is pending;

- It is necessary to retain the data in order to use them as evidence.

Notwithstanding the foregoing, the request to block data will not be granted and any data already blocked may be unblocked if found that the block of data may jeopardize:

- Our performance of the obligations assigned to us by law and/or by the land and any implementing act issued under such law.
- The accomplishment of the objectives that by law fall within the scope of any public interest or the exercise of the processing rights granted us under the laws of Georgia.
- Our legitimate interests or those of any third person except where there is an overriding interest to protect your rights as the data subject, especially a minor.

Well give you a notice of the decision made on your request for data blocking or of the basis for denying such request immediately after such decision is made but no later than 3 business days after you have filed your request for blocking.

**9.1.6** With respect to the data we process automatically when:

- The basis for processing is the consent given by you, or
- The necessity for processing arises from the performance of the obligations under the contract with you as the data subject or from the entry of the contract requested by you, if technically possible, request the receipt, in a structured, generally usable and mechanically readable form, of the data provided by you or release/transmission of such data to any other person (data processor).

**9.1.7** **Withdraw your consent** for the processing of your data at any time, without any explanation or substantiation, and we'll stop processing such data if the processing of the data is based on your consent only.

**9.1.8** Request that where your data, if any, is processed, not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you except where a decision made based on profiling:

- is based on the data subject's explicit consent;
- is necessary for entering into, or performance of, a contract between us;
- is authorized by law.

## 10. Our restriction of your data processing related rights

**10.1** Your rights set forth in Article 9 may be restricted if such a restriction is expressly provided for by the legislation of Georgia, respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard and the exercise of such rights may jeopardize:

1. The interests of national security, information security and cyber-security and/or defense;
2. The interests of public security
3. The prevention, investigation, detection or prosecution of criminal offences or the administration of justice, enforcement of detention and imprisonment, enforcement of non-custodial sentences and probation, crime detection operations;

4. Other important objectives of general public interest, in particular important economic or financial interests of the State (including monetary, budgetary and taxation matters), public health and social security;
5. Detection and prosecution of breaches by the data subject of ethics for professions, including regulated professions;
6. Regulatory and monitoring functions connected to the exercise of official authority in the cases referred to in subparagraphs 1, 2, 3, 4, 5, 7 or 9 of paragraph 10.1.
7. The protection of the rights and freedoms, including the freedom of expression of the data subject and/ or of others;
8. The protection of State, commercial, professional and other secrets envisaged by law;
9. Substantiation of claims or defenses.

**10.2** If the grounds referred to in paragraph 10.1 exist, the data subject will be informed of our decision to restrict the data subject's rights and deny his/her request for the exercise of such rights except where doing so is prejudicial to the accomplishment of the purpose(s) contemplated by paragraph 10.1.

**10.3** In addition to the circumstances referred to in paragraph 10.1, should the data subject file requests unreasonably frequently, we may deny such requests by giving the data subject a prompt written notice thereon, informing him/her of his/her right to appeal.

## 11. Mandatory data processing

**11.1** As part of the products and services we offer you and provide you with, we as the data processor request, subject to the applicable laws, that you provide us with certain data other than those collected/obtained directly from you. As part of the services provided to you, we generate and produce certain data based on the data we have obtained from you just as we receive data from third persons in certain cases.

**11.2** If in the course of the provision of any product or service from us the processing of certain data arises from a legal requirement, aside from our legitimate interest, such as where the data processing is necessary to perform the obligations under a contract with the data subject or to enter a contract at the data subject's request (Article 5(1)(b) of the Law on Personal Data Protection), or if the data processing is authorized by law (Article 5(1)(c) of the Law on Personal Data Protection), your request, in particular, that we: 1. stop processing, delete or erase; 2. block data will automatically result in our termination of the contract and suspension of the relevant services, with a notice thereon to be given you prior to such suspension.

**11.3** You may object to the processing of certain data in cases where such data processing is based on your consent.

**11.4** When we process data subject to legal requirements, your request for deletion or erasure of data will not be granted, as we are required to retain such data in the manner and to the extent defined by law. As for your request for stopping the processing of data, if the processing of such data arises from legal requirements, the data processing will be stopped but we remain bound by law to retain such data in the manner defined and to the extent permitted by law.

## 12. Right to appeal

**12.1** In the event of any breach of this Policy or the rights and rules defined by the applicable laws, you have the right to apply to our Data Protection Officer and, if based on the decision made by us following your application to the Data Protection Officer you still believe that your rights have not been duly realized or the rights breached were not restored, you have the right to duly apply to the Personal Data Protection Office or the court.

**12.2** If you so elect, you also have the right to duly apply directly to the Personal Data Protection Office or the court.