FIRSTBANK

Notice regarding the processing pf personal data

- Mobile banking -

I have read and understood the information on the protection of personal data.

First Bank SA. (hereinafter “First Bank” or the “Bank”), a company existing under the law of Romania, having its registered office in 29-31 Nicolae Titulescu Street, sector 1, Bucuresti, registered with Romanian Trade Registry Office under number J40/1441/27.02.1995, tax registration code 7025592, as Data Controller shall, in accordance with the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“EU General Data Protection Regulation” or GDPR) and the Law no. 190/2018 regarding the implementation of the EU General Data Protection Regulation, process your personal data in good faith and for the purposes specified herein.

1. Personal Data. In order to enroll you for the usage of the 1st Step application (on boarding process) and to provide you the services available through the 1st Step application (i.e. current account service, debit card service and internet banking service, hereinafter generally called "Services"), and considering the purposes of personal data processing mentioned in Section 2, the Bank will process the following personal data:

a) If you are not a client of our internet banking service ("New client")

- your identification data, i.e. your name, address, date and place of birth, unique registration number, your ID number, your nationality and citizenship as well as all the other data included in your ID;

- a copy of your ID;

- your contact data, i.e. your phone and fax number, your e-mail addresses;

- your face image (from ID, selfies and short records using your mobile phone/tablet camera);

- IP, the devise code for the equipment that you use to sign in in Mobile Banking;

-biometric data, i.e. your facial biometric image;

- your voice;

- your job and the nature of your activity, the source of your funds;

- information about the identity of the real beneficiary;

- your reason for opening the current account;

- your estimation regarding the volume of your transactions;

- the Bank's products that you choose to be provided with, IBAN account;

- the OTP (One Time Password);

- your username/User ID and password,

- Mobile Phone name (device name)

- the type of native biometric authentication of the phone/tablet and / or the hash login PIN in the application

- information regarding whether you are subject to the Foreign Account Tax Compliance Act (FATCA);

- information regarding your successful onboarding;

- the advertisement ID of your device (the advertisement IDs represents individual, non personalized and non-permanent identification numbers for devices, provided by iOS, Android or Hyawei).

Based on the personal data you provide us, we will collect information regarding the international sanctions applied to you in the field of anti-money laundry and preventing financing terrorism, if any, as well information regarding your quality of political exposed person, if the case may be.

b) If you are already a client of our internet banking service ("Existing client")

If the Bank identifies you as an Existing client based on your name, e-mail address and your phone number, the Bank shall process for the on boarding purpose only your name, e-mail address, mobile number, your username/User ID and your password, your IP, the device code for the equipment that you use to sign in in Mobile Banking and if the case the number and the expiry date of the card attached to your existing account within First Bank and the CVV2 value. For the acquisition of the Services, the data listed under letter a) are also processed.

If not, the Bank will process all the above mentioned personal data as well for the onboarding.

2. Purposes of personal data processing. Your personal data will be processed by First Bank for the following purposes:

- for on boarding purposes, in order to acquire the Bank services, based on art. 6 (1) letter b) of the GDPR;
- for checking and validating your identity using biometric data, by comparing your face image from the ID with the pictures of your face taken through your mobile phone/tablet, based on your consent according to art. 6 (1) letter a) in conjunction with art. 9 (2) letter a)of the GDPR;

- for checking and validating if you are already our client, based on art. 6 (1) letter f) of the GDPR, in order to facilitate the acquisition of the services;
- for validation of your services request, for fraud prevention, and know your customer purpose, the session, including your face and voice, will be recorded based on art. 6 (1) letter f) of the GDPR,
- for being subject to a decision made exclusively on the automated means that may produce legal effects or which may have similarly significant effects on you, in the meaning that if your identity validation fails, the onboarding process is stopped or in the meaning that if your identity is accurately validated and there are no other reasons to reject you application (i.e. you fulfill the conditions for opening an account, as set below, and you are not in an official databases for international sanctioning lists or in the Metropolitan Police list), the bank account is opened through the means of the Mobile Banking application, based on your consent according to art. 6 (1) letter a) in conjunction with art. 22 (2) letter c) of the GDPR;
- for observing the legal obligations in the field of know your customers, anti-money laundry and preventing financing terrorism, based on art. 6 letter c) of the GDPR;
- for fraud prevention, including by interrogating official databases, as the international sanctions list based on art. 6 letter c) of the GDPR and as the Metropolitan Police data bases, based on or art. 6 letter f) of the GDPR
- for our legitimate interest, respectively for ensuring the security of our IT systems, according to art. 6 (1) letter f) of GDPR
- for marketing direct and/or profiling for marketing purposes, based on your consent according to art. 6 letter a) of the GDPR.

In relation to the personal data processing that may conduct to a decision made exclusively on the automated means, in relation to the validation of the data subject identity, and the anti-money laundering measures, please see the details below:

As confirming that the ID is authentic, we need to confirm that the user presenting the ID is its authorized owner. To prove ownership, we can compare a live capture of the user with the ID photo to confirm facial similarity. Facial recognition is a way of recognizing a human face through technology. A facial recognition system uses biometrics to map facial features from a photograph or video and compare them with a known result (in this case the photo from the ID)

The Face Biometrics feature asks users to perform a randomized sequence of actions during the verification process, to prevent even the most sophisticated spoofing attempts. Our Facial Check with Video provides added security at the point of new user sign-up. The check, available via our partner Onfido Gmbh. (Onfido), prompts users to film themselves repeating numbers and performing randomized movements. Using machine learning, the short video is then checked for similarity against the image of a face extracted from the user's identity document. Crucially, the Facial Check with Video detects liveness, so facial checks can't be spoofed by fraudsters using a stolen photo or identity document.

Your consent will be required in a granular manner for all 3 purposes that are included in this process (each purpose requires a separated consent by ticking one of the

below given boxes) : (i) for data biometrics used for the unique identification of the data subject; (ii) for the recording of the session – your voice and physical body, as your face, and (iii) for processing your personal to make a decision based solely on automated processing, that will produce legal effects for you in the meaning that you will have the possibility to open a bank account (and be provided with a debit card) by using our Mobile Banking application.

In the case that you do not agree with the processing of your biometric data as mentioned above, your on boarding process will stop and you may be able to benefit by the Services by visiting one of our branches.

At the same time, if you give your consent for the processing, please be advised that you have the right to withdraw your consent at any time; the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Also, the Bank may automatically decide that you pose a fraud or money laundering risk if:

- our processing reveals your behavior to be consistent with that of known fraudsters or money launderers; or

- you appear to have deliberately hidden your true identity.

In case your identification fails, or the your name appears on the international sanctions lists or on the Metropolitan Police list or you do not fulfill the criteria for opening an account through the Mobile Banking (please see those criteria below), or there are suspicious for fraudulent behavior, **your registration will be stopped.** You are invited to visit one of our branches to be able to request the banking services and discus with our personnel.
In plus, Banca permite Onfido Gmbh. sa prelucreze datele si in vederea imbunatatirii procesului de invatare automata, pentru scopul prevenirii fraudelor, in temeiul art. 6 alin. 1 lit. f) din GDPR (interes legitim) (a se vedea si sectiunea 7 de mai jos).

Criteria for product eligibility that you need to fulfill: (i) Romanian citizenship; (ii) Able to speak Romanian language; (iii)Age: minimum 18 years old; (iv) Having fiscal residence in Romania; (v) you are not a political exposed person according to Law 129/2019; (vi) you are not listed in an official databases with international sanctions or in Metropolitan Police databases. Also, please be informed that if you are subject to FATCA, we may not onboard you online.

3. Processing the data for marketing and profiling purposes

If you agree to the processing of your data for the purpose of marketing profiling, we will examine the data and information we have available about you to determine what products, services and offers may be useful to you or you may be interested in, what products and services we can develop to meet the wishes and needs of customers, respectively what are the most effective ways and periods for communicating with

you. In this respect, we will process both data that you provide us directly (e.g.: when initiating the contractual relationship, updating your data, purchasing new products and services), and data that we observe during the use of our services (e.g.: data related to the use of the mobile banking application)

The data will be analyzed on the basis of profiling mechanisms that include, in some cases, automated decision-making algorithms related to products / services / events that may be of interest to you. We always ensure that these processing is carried out in compliance with your rights your freedoms and that the decisions made under them have no legal effect on you and do not affect you in a significant way.

If you agree to the processing of your data for marketing purposes, we will communicate you marketing messages with our offers, products and services that we believe may be useful to you.

Both profiling and communication of marketing messages, we can achieve them directly and / or through our partners, including through social networks.

Regarding your profiling through partners, we mention that the Bank uses in its mobile banking application so-called SDKs (Software Development Kit) provided by Facebook (Facebook Inc, 1 Hacker Way, Menlo Park, CA 94025) and Google (Google LLC, 1600 Amphitheater Parkway, Mountain View, CA 94043, USA. These kits transmit pseudonymized data to Facebook / Google, such as the IP address of your terminal, the advertising ID provided by the operating system (IDFA or GAID) and the information that you have completed the enrollment process in the mobile banking application. The information is collected by Google / Facebook and is used to transmit the Bank's communications to people who have a profile similar to your profile, in order to improve the efficiency of dissemination models. At the same time, these kits help increase the success of mobile advertising campaigns run through Facebook and / or Google, in the sense that, for example, no ads will be displayed for the application that is already installed on a device.

The Bank and Facebook / Google process the above mentioned data as jointly controllers, according to the provisions of art. 26 of the GDPR.

Regarding the activity of contacting you through partners, if you have agree to the processing of your data for marketing purposes, whether you complete the enrollment process or not, we will process your data for contacting you through the so-called Custom/matched audiences services provided by Facebook and Linkedin. More details about this service are available here (for Facebook) and here (for LinkedIn).

Also, additional information regarding the processing of personal data by Facebook, Google and LinkedIN is available here (for Facebook), here (for Google) and here (for LinkedIN).

We mention that, if you express your consent for profiling and / or marketing, you have the right to withdraw it at any time. The withdrawal of consent will not affect the legality of the processing based on the consent before its withdrawal.

4. Guaranties in relation to automated individual decision-making.

As you are a subject to a decision based solely on automated processing, that may produce effects concerning your request for banking services in our Mobile Banking application, you have the following rights:

- the right to obtain human intervention from an expert of the Bank;
- the right to express your opinion on the reasons that grounded the decision that affects you;
- the right to submit a complaint and have it analyzed by our specialists.

In addition to these rights, you may visit any of our branch to be able to benefit by the Services provided by the Bank.

5. Duration of data processing. In respect of the above mentioned purposes, your personal data will be stored for a limited period of time, in a safe place and in accordance with the legal provisions and requirements as follows:

a) Existing clients and people who start the remote identification process, whether or not they become clients of the Bank following the onboarding proces

The personal data shall be stored:

- for a period of 5 years after the termination of the business relationship with you, if your personal data that are not used for accounting purposes; and

- for a period of 10 years after the end of the year when the last input in the books of accounts related to you is recorded, if your personal data are used for accounting purposes;

- if you give your consent for profiling and / or marketing, your data will be processed for this purpose from the moment when you give your consent until you withdraw it or until the expiration of a period of one year from the date when the contractual relationship with you ends, whichever occurs first;

b) Persons who start the remote identification process, but do not become clients of the Bank following this onboarding process

The personal data shall be storedfor a period of 5 years from the moment when the data are collected;

If you have given your consent for profiling and/or marketing, your data will be processed for this purpose for a period of 90 days from the time of your consent.-

c) **Persons who do not start the remote identification process (persons in relation to whom the Bank has collected only the email address and telephone number).**

Personal data will be stored:

- for a period of 30 days from the time of data collection; and

- where you have consented to profiling and/or marketing, for a period of 90 days from the time of consent.

However, in some circumstances, for grounded reasons (e.g. legal obligation in this respect, necessity of establishing, exercising and/or defending its rights in front of the courts) the Bank may keep data longer.

6. Data recipients. In order to achieve the processing purposes, First Bank may disclose certain categories of personal data to certain categories of recipients, as follows:

- contractual partners, such as providers of identification and fraud prevention services (e.g. Onfido), services, consultants, bailiffs, public notaries, debt collection or recovery agencies, postal services providers, IT services providers, archiving services providers and any other services providers that are obliged to keep the confidentiality of the data; the list of Onfido subcontractors cand be accessed here

- judicial authorities or other public authorities, such as national Bank of Romania, National Office for Prevention and Control of Money Laundering, Financial Supervisory Authority, National Agency for Fiscal Administration, Metropolitan Police, etc.

7. Machine Learning

Your personal data is used by Onfido Gmbh. (https://onfido.com), as an independent data controller, for the purpose of improving the machine learning process in order to prevent fraud, pursuant to Article 6 para. 1 lit. f) of the GDPR (legitimate interest). Onfido is a company established and registered in Germany, and with company registration number HRB133755, headquartered at Am Kaiserkai 69, 20457 Hamburg.

Onfido limits the processing to the technical elements of the ID card (structure of the ID card), the data in your ID card and your photo. Information on the processing of your data by Onfido is available here.

To exercise your rights with regard to the processing of personal data for the purpose of improving the machine learning process, you can contact:

- Onfido at privacyrequests@onfido.com;

- First Bank, at 29-31 Nicolae Titulescu Street, sector 1, Bucuresti, office@firstbank.ro.

8. Transfer of personal data.

In the event that your personal data shall be transferred out of the UE/EEA to data recipients in third countries which do not ensure an adequate level of data protection as determined by the European Commission, the transfer shall be done based on the European Commission approved Standard Contractual Clauses or other data protection safeguards in compliance with Privacy Laws. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries(https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en).

9. Your rights in respect of the processing of your personal data. We also inform you that, in accordance with Article 12-22 of the GDPR, you have the following rights: (i)The right to information and access to your personal data, (ii)The right to have your personal data rectified, (iii)The right to be forgotten/to have your personal data erased, (iv)The right to restriction of processing; (v)The right to data portability; (vi)The right to object to the processing of your data, if your personal data are processed pursuant to Article 6 (1) (e) or (f) of GDPR, and for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and for the purposes of the legitimate interests pursued by the Controller (vii) The right not to be subject to an individual decision, meaning that you have the rights provided in Section 4. (viii) the right of withdrawing your consent for the processing performed based on it.

In order to exercise these rights, you may send a dated and signed written request to First Bank, 29-31 Nicolae Titulescu Street, sector 1, Bucuresti or by e-mail to office@firstbank.ro or dpo@firstbank.ro.

Your request will be analyzed and answered without delay, but in any case, not later than one month from receipt of such request.

You also have the right to refer a matter to the National Supervisory Authority for Personal Data Processing or to any competent courts.

10. Other aspects. The data controller guarantees that your data are processed for legitimate purposes, and that it implements adequate technical and organizational

measures to ensure data integrity and confidentiality pursuant to Articles 25 and 32 of the EU General Data Protection Regulation.