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;

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

- 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 and legal grounds of personal data processing. Your personal data will be processed by First Bank for the following purposes:

a) for on boarding purposes, in order to acquire the Bank services, based on art. 6 (1) letter b) of the GDPR;
b) for checking and validating your identity using biometric data, by comparing your face image from the ID with the images of your face taken with your mobile phone/tablet/camera, and also for comparing your biometric data with the biometric data of clients already enrolled in the First Bank remote identification system, based on your consent according to art. 6 (1) letter a) of the GDPR in conjunction with art. 9 (2) letter a) of the GDPR;
c) for verifying the fulfillment of eligibility conditions necessary for initiating the contractual relationship, as mentioned in the Terms and Conditions of service provision, based on Article 6(1) letter b) of the GDPR.

Note: For the purposes mentioned above, the Bank uses an automated decision-making process that can produce legal effects or may have significant effects on you. Thus, if the validation of your identity fails or the eligibility conditions are not met, the registration process is halted. The decision-making process is based on article 22(2) letter a) of the GDPR (in the case of identity verification and validation), and article 22(2) letter c) of the GDPR (verification of fulfilling the eligibility conditions).

d) for checking or validating whether you are already our client, based on Article 6(1) letter f) of the GDPR, to facilitate the acquisition of services;

e) for complying with legal obligations in the area of knowing your customer, preventing money laundering, and combating the financing of terrorism, including for FATCA reporting, based on Article 6 letter c) of the GDPR;
f) for fraud prevention, including by querying official databases, under Article 6 letter c) of the GDPR;
g) for our legitimate interest in ensuring the security of our IT systems, according to Article 6(1) letter f) of the GDPR;
h) for our legitimate interest in identifying fraud attempts and improving the systems for preventing them, according to Article 6(1) letter f) of the GDPR;
i) for direct marketing and/or profiling for marketing purposes, based on your consent, according to Article 6 letter a) of the GDPR.

In addition, Onfido GmbH processes your data for the purpose of improving identification and fraud prevention systems, under Article 6(1) letter f) of the GDPR (legitimate interest) (see also section 7 below).

Data Processing for Remote Identification

Based on your consent, the photograph of your ID will be compared to a "selfie" photo that includes your facial features, taken with the help of a smartphone/camera, via a facial biometrics application provided by an external contractor (Onfido GmbH). For this comparison, the application will create two biometric models based on the features of your face as it appears in the two images. The features analyzed for creating the biometric models include the shape of the eyes, eyebrows, lips, nose, and jaw, the texture of the skin, and any moles or wrinkles. Following the automated comparison process, the facial identification tool will issue a similarity score. The higher this score, the greater the probability that the face in the two images belongs to the same person.

If you do not agree with the processing of your data as described above, your registration process will be stopped, and you will be able to get the services by visiting one of our branches. At the same time, if you give your consent for processing, please note that you have the right to withdraw your consent at any time; withdrawing consent will not affect the lawfulness of processing based on consent before its withdrawal.

Your ID copy will be verified, through the Onfido GmbH app, from the perspective of forgery risk, to confirm its validity. In this regard, the Bank will analyze the format, appearance, and integrity of the data included in your ID.

“Known Faces” Feature

To prevent fraud, the Bank utilizes the "Known Faces" feature. This functionality involves comparing the biometric data mentioned above, belonging to a client undergoing the remote identification process, with the biometric data of clients already enrolled in the First Bank remote identification system. Thus, upon enrollment, the photograph or video that includes your face is uploaded into a dedicated database, and your biometric data are compared with that of already enrolled clients. Subsequently, your data will be retained in the database and will be compared with the data of new users to minimize the risk that a third party could identify themselves with a counterfeit document containing your data. Each new check stores the used photo/video image in the database.

For data minimization and security, pseudonymization technologies known as "embedding" are used, which transform the person's image into biometric numeric identifiers. Thus, the comparison is made between biometric numeric identifiers, and not between actual images.

If you do not agree with the processing of your data as described above, your registration process will be stopped, and you will be able to receive services by visiting one of our branches. At the same time, if you give your consent for processing, you can change your mind at any time by writing to the contact addresses provided in this notice; in this situation, we will remove your data from the aforementioned database. Withdrawing consent will not affect the lawfulness of processing carried out before the withdrawal.

“Repeated Attempts" Feature

This technical solution involves comparing the data from the identity document of a client undergoing the remote identification process with the data of clients already enrolled through the First Bank remote identification system. This functionality reduces the risks of identity fraud by recognizing situations where a document is reused with variations in identity information. "Repeated Attempts" builds a database with data extracted from identity documents and the conclusions of identity document verifications, so that when a new document check is performed, a search is conducted to identify possible matches.

Automated Decision-Making Process

For initiating a contractual relationship remotely, the Bank uses an automated decision-making system for:

- your identification, by using your data, as detailed above; and

- verifying your data against international sanctions lists; and

- checking the fulfillment of the eligibility criteria mentioned in the Terms and Conditions of Service provision.

If your identification fails, or your name appears on international sanctions lists, or you do not meet the eligibility criteria, the remote enrollment process will be stopped. In this case, you are invited to visit one of our branches to request banking services and discuss with our staff.

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 process

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 6 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 stored for 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.

d) The photographs/videos used for the purpose of the "Known Faces" feature will be processed for a period of up to 90 days from the date of their collection. Biometric identifiers will be retained for a period of no more than one year from their collection.

e) The data used for the purpose of the "Repeated Attempts" feature will be processed for a period of up to 90 days from the date of their collection.

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, etc.

7. Identification of fraud attempts and improvement of Onfido's fraud prevention systems

Your personal data are used by Onfido GmbH (https://onfido.com), as an independent data controller, for the purpose of improving the identification and fraud prevention system, including through machine learning, under Article 6(1) letter f) of the GDPR (legitimate interest). Onfido GmbH is a company established and registered in Germany with company registration number HRB 211512 B, headquartered at Am Kaiserkai 69, 20457 Hamburg.

In this regard, Onfido processes the following personal data: your photograph, the data from your identity document, your phone number, the unique identification code assigned by Onfido, the results of verifications carried out by Onfido, and any other information that you provide us during the identification process or that we collect through observing your activity via the devices you use in the identification process (e.g., IP address, traffic or location data, logs). Additionally, Onfido may process information regarding users identified by the Bank as fraudulent. Information on the processing of your data by Onfido is available here (https://onfido.com/privacy/).

To exercise your rights regarding the processing of personal data by Onfido, including the right to object to the processing of data for the purpose of improving the machine learning process, you can contact Onfido at privacyrequests@onfido.com. Onfido's Data Protection Officer can be contacted at the same address.

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.

In accordance with the Terms and Conditions of using the internet/mobile banking service, which have been made known to you, we note that the Mobile Banking online enrollment platform cannot be accessed if you are located within the U.S.A.

We wish to clarify that if you nevertheless access the remote enrollment process from the territory of the United States of America, the personal data you provide during this process, including biometric data, will be processed by Onfido, based on the consent you expressed at the initiation of the enrollment process, in accordance with:

(i) legislation regarding biometric information, including the Illinois Biometric Information Privacy Act (BIPA) - for those accessing the platform from the USA;

(ii) European legislation on the protection of personal data;

(iii) Onfido's Facial Scan Policy (https://onfido.com/facial-scan-policy-and-release/);

(iv) Onfido's Developer Guides (https://developers.onfido.com/guide/onfido-privacy-notices-and-consent);

(v) Onfido's Terms of Service (at https://onfido.com/terms-of-service/).