

Notice regarding the processing of personal data

–personal data update –

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

1. First Bank S.A. ("First Bank" or "Bank"), as a financial banking institution, processes the following data concerning you, in accordance with the requirements of the legislation in the field of knowing the clientele and the prevention and laundering of money, respectively the fight against terrorism:
 - 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 number and your e-mail addresses;
 - biometric data (your facial biometric image) and your voice, in case there are changes to your data;
 - your occupation and the nature of your activity/the duration of the employment contract, the source of your funds;
 - the purpose and nature of the business relationship with the bank;
 - falling into the category of publicly exposed persons or being a family member of a publicly exposed person or a person known as a close associate of a publicly exposed person (PEP);
 - information about the identity of the real beneficiary;
 - information regarding whether you are subject to the Foreign Account Tax Compliance Act (FATCA);
 - information regarding the possible international sanctions that are applied to you in the field of combating money laundering and preventing the financing of terrorism;
 - the OTP (One Time Password).

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

- a) in order to update the data, to comply with the legal obligations in the field of knowing the clientele, preventing money laundering and combating the financing of terrorism, including with a view to FATCA reporting, pursuant to art. 6 letter c) of the GDPR;

- b) for the verification and validation of your identity using biometric data, by comparing the image of your face on the identity card with the images of your face taken with the mobile phone/tablet/video camera, 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 - if there are changes to your data;

So, based on your consent, your ID photo will be compared with the "selfie" photo that includes your physiognomy, taken with your smartphone/video camera device, through a facial biometrics application provided by a contractor external (Onfido Gmbh). In order to make this comparison, the application will create two biometric models based on the characteristics of your face, as it appears in the two images. The characteristics that will be analyzed in order to create the biometric models include the shape of the eyes, the eyebrows, the shape of the lips, the nose, and the jaw, the texture of the skin, any moles or wrinkles. Following the automatic comparison process, the facial identification tool will issue a similarity score. The higher this score, the higher the probability that the face in the two images belongs to the same person. This verification process is automatic and may stop the data update process if your identity validation fails. The decision-making process is based on art. 22 (2) lit. a) GDPR.

If you do not agree with the processing of your data according to the above, your data update process will be stopped and you will be able to update your data by visiting one of our branches.

- c) for our legitimate interest in identifying fraud attempts and improving their prevention systems, according to art. 6 (1) lit. f) from GDPR;

The copy of your identity document will be checked, through the Onfido Gmbh application, from the perspective of the risk of counterfeiting, in order to confirm its validity. In this sense, the Bank will analyze the format, appearance and integrity of the data included in the identity document.

- d) for direct marketing and/or profiling for marketing purposes, based on your consent, according to art. 6 letter a) of the GDPR.

In addition, Onfido Gmbh processes your data in order to improve the fraud identification and prevention systems, under to art. 6 para. 1 lit. f) from the GDPR (legitimate interest) (see also section 7 below).

3. Automated Decision- Making Process

In order to identify you as detailed above, and to verify your data in the lists of international sanctions, the Bank uses an automated decision-making system.

If your identification fails or your name appears on international sanctions lists, the remote enlistment process will be stopped. In this case, you are invited to visit one of our branches to be able to request banking services and talk to our staff. The processing of your data through the automated process is based on art. 22 (2) lit. b) and c) GDPR.

Since you are subject to a decision based exclusively on automatic processing, which may have effects on your request for banking services in our Banking Mobile application, you have the following rights:

- the right to obtain human intervention from an expert of the Bank;
- the right to express your opinion regarding the reasons that substantiated the decision that affects you;
- the right to file a complaint and receive an analysis from our specialists.

4. Processing the data for marketing and profiling purposes

In the situation that you express your agreement regarding the processing of your data for the purpose of marketing profiling, we will examine the data and information we have about you in order to understand what products, services and offers may be available to you, useful or may interest you, what new products and services we can develop to meet the wishes and needs of customers, respectively what are the most effective ways and periods of communication with you. In this sense, we will process both data that you provide us directly (e.g.: on the occasion of initiating the contractual relationship, updating data, purchasing new products and services), as well as 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 based on profiling mechanisms that include, in some cases, automated decision-making algorithms in relation to the products/services/events that may be of interest to you. We always ensure that these processes are carried out in compliance with the rights and your liberties and that the decisions made based on them do not have legal effects on you and do not similarly affect you to a significant way.

If you agree to the processing of your data for marketing purposes, we will send 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.

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:

Personal data will be stored for a period of 5 years from the date of termination of the business relationship with you according to the legal norms applicable in the financial and accounting field. In the situation where you have expressed your consent for profiling and/or marketing, your data will be processed for this purpose from the moment you express your consent and until its withdrawal or the expiration of a period of one year from the date of termination of the contractual relationship, whichever the first of these intervenes.

However, in certain circumstances, if there are thoroughly justified reasons (eg: the existence of a legal obligation, the need to establish, exercise or defend the Bank's rights), the Bank can keep the data for a longer time.

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 can be accessed [here](#).
- members of the Intesa Sanpaolo banking group;

- 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 \(https://onfido.com/privacy/\)](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/dataprotection/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.

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-notice-and-consent/>);
- (v) Onfido's Terms of Service (at <https://onfido.com/terms-of-service/>).

This information note is supplemented with the provisions of the general information note regarding the processing of personal data of natural persons, available at www.firstbank.ro, Data Protection section, which we recommend you to consult.