GENERAL PRIVACY NOTICE REGARDING THE PROCESSING AND PROTECTION OF PERSONAL DATA BELONGING TO BT CUSTOMERS

Version applicable from October 24, 2023

BANCA BT TRANSILVANIA®

Table of Contents

I. About this Privacy Notice and our commitments

This privacy notice is addressed to BT Customers ("**Customers**" or "**BT Customers**") - as defined in section II - and represents the way in which **Banca Transilvania S.A.** (" **the Bank**", "**BT**", "**we**") fulfills its obligation to inform them in regard to the processing of their personal data ("**personal data**", "**data**").

We provide you with this privacy notice in accordance to art. 13-14 of the General Data Protection Regulation ("**GDPR**"), so that you are transparently informed about the processing that BT carries out on your personal data when you become a BT Customer, throughout the period that you have this quslity, as well as for certain periods imposed by law after you cease to be a BT Customer.

This notice is general in nature and forms an integral part of the BT Privacy Policy. You can find the Privacy Policy as well as this general privacy notice both on the BT website https://en.bancatransilvania.ro/ (including in the **Privacy Hub** section on this website), as well as in BT units.

For certain services/products/personal data processing activities that we carry out, we have prepared specific privacy notices, which you can find in the **Privacy Hub** section.

We comit to process and protect your personal data in compliance with the applicable legal provisions and the highest security and confidentiality standards, to respect the fundamental human rights and freedoms in regard to this processing and to regularly assess our activity in this field, to make sure these rights are always respected.

For guidance and support of our personal data processing and protection activity we have appointed a data protection officer ("**DPO**"). BT's DPO can be contacted by any data subject, at any of the following contact data:

- the e-mail address dpo@btrl.ro.
- the Bank's headquarters in Cluj-Napoca, Calea Dorobanţilor, no. 30-36, Cluj County, Romania, with the specification: "to the attention of the data protection officer".

We comit to periodically review this privacy notice and to inform you of any material changes made to it, by means of direct communication (via the secure messaging of the Neo BT or BT24 internet banking service - if you use these BT services - or by message to the e-mail address or phone number declared at BT - if you do not use the internet banking services and you have declared at least one of these contact details at the bank) and/or indirectly (e.g. by making available of the updated version of the privacy notice in all BT units and on the BT website).

We further present to you who BT is (the data controller), what categories of personal data we process for BT Customers (the data subjects that we refer to in this privacy notice), for what

purposes we use this data, to whom we can disclose or transfer it, how long we keep them, as well as what rights can Customers exercise in connection with this processing.

If you are not familiar with the meaning of different specialized terms used in the GDPR or the applicable banking law, we recommend that you first read section A of the BT Privacy Policy.

II. Who is a BT Customer

In this privacy notice, the data subjects who are subject to the processing of personal data are BT Customers, defined as follows.

"**BT customer**" or "**Customer**" means any of the below mentioned categories of data subjects:

➢ resident/non-resident individuals, holders of at least one current account opened with the bank (also referred to as "BT individual account holder") or persons who rent safe deposit boxes at BT;
➢ legal or conventional representatives of the BT individual/legal entities account holders or who rent deposit boxes;
➢ individuals authorized to perform operations on the accounts of BT individual/legal entities account holders ("mandated person");
➢ the real beneficiaries of Customers who are individual or legal entity BT account holders ("beneficial owner");
➢ individuals with rights to submit bank documents, to pick up account statements and/or to make cash deposits on behalf of BT individual/legal entities account holders ("delegates");
➢ associates/shareholders of some BT Clients legal entities;
➢ users of a product/service of the bank who do not have any of the qualities mentioned above but they regularly use some BT products/services (e.g. users of additional cards, individuals with account manager's securities records opened with the bank, BT meal tickets users, users of BT Pay);
➢ guarantors of any kind of the payment obligations assumed by the individuals/ legal entities account holders;
➢ persons who sign the bank's dedicated request forms to become BT Customers, but this request is rejected or waived (even if these individuals are not active BT Customers, we are bound by law to keep their personal data for a certain period of time);
➢ the legal or conventional successors of the aforementioned.

III. Who is the controller of the personal data

BANCA TRANSILVANIA S.A. is a credit institution, Romanian legal entity, registered with the Trade Register under no. J12/4155/1993, tax identification number RO 5022670, with the following address: registered office in - Cluj-Napoca, Calea Dorobanţilor, no. 30-36, Cluj County, phone no. *0801 01 0128 (BT) - Romtelecom network, 0264 30 8028 (BT) - any

network, including international calls, *8028 (BT) - Vodafone, Orange network, e-mail address: contact@bancatransilvania.ro, website BT: https://www.bancatransilvania.ro/.

Banca Transilvania S.A. is the parent company of the BT Financial Group.

The provisions of this privacy notice refer to the processing of personal data that BT carries out as a controller.

In some of our activities we process personal data as joint controllers, together with other entities. You can find details about this processing in the specific privacy notices found in the **Privacy Hub** section on the BT website.

IV. Purposes for which we process personal data of Customers

As a BT customer, we process your personal data, upon case, for:

➢ applying the know your customer (KYC) measures in order to prevent money laundering and terrorism financing. Details in the specific privacy notice in the **Privacy Hub**;
➢ assessing the solvency, reducing the credit risk, determining the degree of indebtedness of the Customers interested in personalized offers in relation to the bank's credit products or in contracting these types of products (credit risk analysis), including by processing the personal data in the Credit Bureau system. Details in the specific privacy notice in the **Privacy Hub**;
➢ the conclusion and performance of contracts related to products/services offered to BT customers (such as, but not limited to: debit/credit cards, deposits, credits, internet and mobile banking, BT Pay, SMS Alert); Details on the processing of personal data for some BT products/services can be found in the specific privacy notices in the **Privacy Hub**;
➢ the conclusion and performance of contracts for occasional transactions (please see section C point 2 of the BT Privacy Policy when you act as a walk-in client even if you are also a BT customer);
➢ processing/settlement of the banking transactions;
➢ establishing the garnishments, recording the amounts garnished to the creditors and providing answers to the enforcement bodies and/or the competent authorities, according to the legal obligations of the bank;
➢ reporting to the competent authorities, in accordance with the legal obligations that the bank is subject to (e.g. reports to the National Administration of Public Finances – A.N.A.F., National Bank of Romania -N.B.R.- including to the National Office for Prevention and Control of Money Laundering, the Central of Credit Risks and the Office of Payment Incidents within N.B.R. etc);
➢ conducting analyses and the keeping of records for the Bank's economic, financial and/or administrative management;
➢ management within the internal departments of the services and products provided by the Bank, as well as management of the human resources;
➢ debt collection and recovery of receivables;

➢ defending the bank's rights and interests in court, the resolution of disputes, investigations or any other petitions/ complaints/requests in which the bank is involved;

➢ performing risk controls on the bank's procedures and processes, as well as carrying out audit or investigation activities, including for the prevention and management of conflicts of interest;

➢ taking measures/providing information or answers to the requests/claims/complaints of any nature addressed to the bank by any person, including by legal authorities or institutions. For details on the processing of your data, if you have addressed such petitions to the bank, please also study section C point 10 of the BT Privacy Policy;

➢ proving the requests / agreements / options regarding certain aspects requested / discussed / agreed upon via the phone calls initiated by the Customers or by the bank, by taking notes of the discussed issues and, as the case may be, the audio or video recordings of the phone calls or the video calls;

➢ informing the Customers in regard to the products/services held with the bank, for the proper execution of the contractual relationship (this is done, upon case, through messages of general or particular interest addressed to the Customers such as, but not limited to: transmitting of bank account/card statements, transaction reports, notices regarding garnishments on the accounts, notifications for unauthorized debits or overdue payments of installments, notices about the approach of the contractual term for a particular product/service held, notices about improvements or new facilities offered in relation to the product/service held, about the modification of the general business conditions or the general privacy notice regarding the processing of personal data, about the need to update the data etc.);

➢ sending marketing messages/commercial communication to Customers who have consented to have their personal data processed for this purpose. For details about the processing of your data, if you have expressed options regarding the processing of your data for marketing purposes at BT, please also study section C point 12 of the BT Privacy Policy;

➢ evaluating/improving the quality of services (requesting/collecting the opinion of Customers regarding the quality of BT services/products/employees);

➢ the Customers' financial education;

➢ conducting internal analyses (statistics included) both with regard to products/services and the Customers profile and portfolio, market research, customer satisfaction analysis for the Bank's products/services/employees);

➢ development and testing of BT products/services;

➢ archiving in physical/electronic format of documents/information, including back-up copies;

➢ the performance of registration and secretary services regarding the correspondence addressed to the bank and/ or sent by it;

➢ ensuring the security of the IT systems used by BT and of the premises in which the bank operates its activity;

➢ monitoring the security of persons/premises/assets of BT and of the visitors of BT units/equipment. Details about the processing of personal data in this purpose can be found in the specific privacy notice regarding video surveillance as well as in the specific privacy notice referring to visits in some of the BT offices, in the **Privacy Hub** section.

➢ fraud prevention;

V. What data of BT Customers we process

We process the following categories of personal data belonging to BT Customers, upon case:

➢ **identity data**: name, surname, alias (if applicable), date and place of birth, national identification number (Romanian national identification number - "cod numeric personal"- C.N.P.) or another unique similar identification element (e.g. CUI for authorized natural persons or CIF for natural persons carrying out liberal professions -professionals), other details from the ID document/passport, as well as a copy such documents, signature (handwritten or electronic), citizenship, domicile and residence address as well as the address where the Customer lives and its legal regime;

➢ **contact data**: phone number, e-mail and correspondence address, fax;

➢ **financial data** (such as, but not limited to: transactions, data on the payment behavior, data about accounts and financial/banking products, held with/processed through BT or other financial institutions);

➢ **fiscal data** (e.g. country of fiscal residence, tax registration number);

➢ **professional data** (e.g. profession, job, job title, name of employer or nature of the individual activity, level of studies, specialization, information about the important public position held if you are a publicly exposed person (PEP), the quality, the social parts/shares and, as the case may be, the powers of attorney held within certain legal entities);

➢ **information on the family status** (e.g. marital status, marital regime, number of dependents, kinship relations, marriage, cohabitation);

➢ **information on the economic and financial status** (including data on income, data on owned assets, as well as your wealth's source if you are PEP);

➢ **data about the BT products/services requested/used** (e.g. information about the purpose and nature of the business relationship, the source/destination of the funds used in the contractual relationship/transactions, the type of products/services, the contractual period, other details of the products/services, including, for credit products - the type of product, the granting term, the granting date, the maturity date, the granted amounts and credits, the amounts due, the status of the account, the date of closing the account, the currency of the credit, the frequency of payments, the amount paid, the monthly rate, the name and the address of the employer, the amounts owed, the outstanding amounts, the number of outstanding installments, the due date of the outstanding, the number of overdue days in the repayment of the loan. Data related to credit products are processed both in the bank's own records, and - as the case may be - in the records of the Credit Bureau and/or other records/systems of this type);

➢ **image** (contained in the identity documents or captured by the video surveillance cameras, as well as captured in certain video recordings);

➢ **voice**, within the calls and recordings of the audio/video calls (initiated by the Customers or the bank);

➢ **biometric data** (e.g. face recognition, used in remote identification processes by video means, in methods of unlocking devices on which you have BT apps installed, if you have set

up methods such as facial or fingerprint-based recognition – in the latter case BT does not have access to your biometric data, but only relies on it to allow you to access/use some BT applications);

➢ **age**, to verify the eligibility to contract certain products/services/offers of the bank (e.g. credit products, products dedicated to under-age individuals, etc.);

➢ **opinions**, expressed through notices/complaints or during conversations, including phone, regarding products/services/employees of the bank;

➢ **identifiers**, allocated by BT or by other banking or non-banking institutions, such as, but not being limited to: the BT client code (CIF BT), references/identifiers of transactions, IBAN codes of bank accounts, the numbers of the credit/debit cards, contract numbers, identifiers allocated by the bank to the Customers who are "nonresidents", consisting of a sequence of figures referring to the year, month, day of birth and the number of the identity document), IP addresses, identifiers of the devices (e.g. mobile phones) and of the operating system of the devices used to access mobile banking services/mobile payment applications;

➢ **data concerning health**, if such information is provided to us as part of banking documentation, results from transactions or if the processing of such data is necessary for customers to prove the difficult situation in which they or their family members find themselves, especially with a view to granting facilities for lending products;

➢ **information regarding fraudulent / potentially fraudulent activity**,

➢ **information regarding the location of certain transactions** (implicitly, in case of operations at the ATMs or POS belonging to the Banca Transilvania);

➢ **any other personal data** belonging to the Customers, which are brought to the bank's knowledge in various contexts by other Customers or by any other person.

VI. What are the sources from which we collect personal data of Customers

As a rule, the personal data we process is collected directly from you (e.g. when you become a BT Customer, update your data in the bank's records, perform transactions, you apply for certain products, such as credit products etc.)

However, there are situations when data is collected from other sources, from:

➢ other BT Customers (e.g. authorization of other Customers on their accounts opened at the bank, contracting of some bank products/services by a Customer on behalf of another Customer who authorized him in this regard, contracting by employers who are BT Customers of some products/services of the bank for/on behalf of their employees – meal vouchers, collection of salary income in accounts opened at BT, managed guarantee accounts, etc.);

➢ persons who are not BT customers (e.g. persons who deposit cash amounts in the accounts of BT Customers, persons who send petitions in which they claim to use data declared at the bank by BT Customers);

➢ public authorities or institutions (e.g. The General Directorate for Personal Records - D.G.E.P. - from which we receive current data of the identity document of customers or of people who go through the steps to become BT customers, which we process for the purpose

of knowing the customers according to the details in the **Privacy Hub** section on the website, subsection "Knowing the clientele", courts, prosecutors, police, bailiffs, B.N.R., A.N.P.C., A.N.S.P.D.C.P., etc.), notaries, lawyers;

➢ institutions involved in the field of payment services (e.g. Transfond, S.W.I.F.T, international payment organizations, etc.);

➢ other credit institutions with which Banca Transilvania S.A. merged (Volksbank România S.A. and Bancpost S.A.) or from which some contracts were assigned (Idea::Bank);

➢ other banks/financial institutions, including partner banks and correspondent banks or banks/financial institutions participating in syndicated loans;

➢ other entities of the BT Financial Group, for determined and legitimate purposes, in general for the performance of the financial/economic activity and to fulfill the legal requirements related to the supervision on consolidated basis of the BT Group;

➢ public sources, such as but not limited to: the National Office of the Trade Register (O.N.R.C.), the National Register of Property Advertising (R.N.P.M.), the Office of Cadastre and Real Estate Advertising (O.C.P.I.), the court portal (portaljust), the Official Gazette , social media, internet, etc.;

➢ records of the type of the Credit Bureau, the Credit Risk Center within the B.N.R., if there is a legal basis and a determined and legitimate purpose for their consultation;

➢ database providers (e.g. entities authorized to administer databases with persons accused of financing acts of terrorism, publicly exposed persons, providers that aggregate and redistribute data collected from public sources, etc.);

➢ contractual partners of the bank from various fields (e.g. evaluation companies, insurance companies, pension and investment fund management companies);

➢ debt collection/debt recovery companies (e.g. we can find out the new contact details of the Clients from the companies that support us in the debt recovery activity);

VII. On what legal grounds do we process personal data of Customers and what happens if you refuse their processing

The legal grounds on which BT processes personal data are, upon case:

➢ the legal obligation of the bank (processing is necessary for compliance with a legal obligation to which the bank is subject);

➢ conclusion/execution of contracts (processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract);

➢ the legitimate interest of the bank and/or third parties;

➢ processing is necessary for the performance of a task carried out in the public interest (e.g. application of the know your customer measures to prevent money laundering and terrorist financing);

➢ consent of the data subject.

When we are required by law to process certain data in a certain situation or if your data is necessary to conclude or perform contracts for BT products/services, if you refuse their

processing you will not be able to become/remain a BT Customer or we will not be able to process the transactions you request.

If we process your data for the legitimate interests pursued by us or third parties, you can object to that processing for reasons related to your particular situation (e.g. if you are a BT Customer and no longer wish to receive messages of general interest or messages asking you to rate the quality of our services/products, we will accommodate your request without affecting your business relationship with BT). In some cases, our legitimate interest or that of third parties may prevail over yours and we will not be able to accommodate the request through which you object to the processing (e.g. data processing in the Credit Bureau system, if there are no other reasons for accommodating the opposition request).

If we process your data based on your consent, you have the right to withdraw this consent at any time. However, the withdrawal will not affect previous processing operations performed of your data (e.g. we process your data under consent for marketing purposes and you have the right to withdraw this consent. Withdrawal of marketing consent does not affect your right to become or remain a BT Customer. However, the refusal to have your data processed for marketing purposes means that the bank will not be able to notify you about certain offers/promotions and, as a consequence, it is possible that in some cases you will not be able to benefit from products/services under promotional conditions).

VIII. To whom we may disclose/transfer the personal data of Customers

The personal data of Customers that we process, may sometimes be disclosed/transferred by BT in accordance with the GDPR principles, based on the applicable legal grounds depending on the situation and only under conditions that ensure their full confidentiality and security.

We commit to respect the fundamental human rights and freedoms in the event of such disclosures, in particular the right to the protection of personal data and the right to privacy, and to periodically evaluate our work in this area to ensure that these rights are always respected.

You can find below in this section (* -> ***) details about legal provisions that require us to report/communicate personal data concerning you to some authorities.

Also, when public authorities/institutions request us to provide personal data, we commit to only disclose them if we have a legal obligation or a legitimate interest, only based on clear internal procedures and only with the approval of persons in a management position.

We will only make available to the authorities the strictly necessary data and if it is demonstrated that we have made such disclosures of personal data in violation of human rights, we commit to repair the damage caused to the data subjects.

The categories of recipients to whom we may disclose personal data are, upon case:

➢ other Customers who have the right and need to know them;

➢ other entities within the BT Financial Group;

➢ companies involved in payment processing (e.g.: Transfond S.A., payment processors);

➢ financial-banking entities (e.g. participants in payment schemes/systems and interbank communications such as S.W.I.F.T., S.E.P.A., ReGIS, partner banks and correspondent banks, banks or financial institutions participating in syndicated loans);

➢ international payment organizations (e.g. Visa, Mastercard);

➢ contractual partners (service providers) used in BT's activity, such as but not limited to providers/suppliers of: services for issuing digital certificates (for the application of the qualified/extended electronic signature), overdue/receivables collection services, IT services (maintenance, implementation, support, cloud), services of archiving in physical and/or electronic format, courier, audit, card-related services, market studies/research, e-mail/SMS/phone call transmission, marketing services, other services offered by providers to whom BT has outsourced certain financial-banking services, etc.);

➢ insurance companies;

➢ real estate evaluation companies;

➢ management companies of pension and investment funds

➢ companies (funds) guaranteeing various types of credit/deposit products (e.g. F.N.G.C.I.M.M., F.G.D.B., etc.);

➢ partners of the bank in various fields, whose products/services/events we can promote to BT Customers based on their consent. The updated list of the bank's partners can be found here: https://www.bancatransilvania.ro/parteneri;

➢ assignees;

➢ national public authorities and institutions, such as, but not limited to: the National Bank of Romania (N.B.R.), the National Fiscal Administration Agency (A.N.A.F.)*, the Ministry of Justice, the Ministry of Internal Affairs (M.A.I.), The General Directorate for the Records of Persons (D.G.E.P.) to which we transmit the name, surname and CNP of customers/ persons who go through the steps to become BT customers for the validation of this data and for the provision of additional information from their current identity documents, which we process for the purpose of knowing the customers according to the details in the **Privacy Hub** section of the website, subsection "Knowing the customers", the National Office for the Prevention and Combating of Money Laundering Money (O.N.P.C.S.B.)**, the National Agency for Cadastre and Real Estate Advertising (A.N.C.P.I.), the National Register of Real Estate Advertising (R.N.P.M.), the Financial Supervision Authority (A.S.F), including, as the case may be, their territorial units;

➢ banking institutions or state authorities, including from outside the European Economic Area - in the case of S.W.I.F.T.-type international transfers or as a result of the processing carried out for the purpose of applying F.A.T.C.A legislation. and C.R.S.;.

➢ public notaries, lawyers, bailiffs;

➢ Credit Risk Register***;

➢ The Credit Bureau and the Participants in the Credit Bureau system****;

* disclosing personal data to A.N.A.F.

According to the provisions of the Fiscal Procedure Code (Law no. 207/2015), in its capacity as a credit institution, BT has the legal obligation to:

1. Communicate daily to A.N.A.F.:

- the list of holders of natural persons, legal entities or other entities without legal personality that open or close at BT bank or payment accounts, the persons who have the right to sign for the opened accounts, the persons who claim to act on behalf of the client, the real beneficiaries of the account holders, together with the identification data provided for in art. 15 para. (1) from Law no. 129/2019 for the prevention and combating of money laundering and the financing of terrorism, as well as for the modification and completion of some normative acts, with subsequent amendments and additions, or with the unique identification numbers assigned to each person/entity, upon case, as well as with the information regarding the number IBAN and date of opening and closing for each individual account.

- the list of people who rented safe deposit boxes, accompanied by the identification data provided in art. 15 para. (1) from Law no. 129/2019, with subsequent amendments and additions, or by the unique identification numbers assigned to each person/entity, as the case may be, together with the data related to the termination of rental contracts.

2. Communicate, at the request of A.N.A.F., for each account owner who is the subject of the request, all turnovers and/or balances of the accounts opened at the bank, as well as the information and documents regarding the operations carried out through those accounts.

3. Submit to A.N.A.F. – on occasion of a request to open a bank account or to rent a safe deposit box - the request for the assignment of the fiscal identification number/fiscal registration code for non-resident natural persons that do not have a fiscal identification code. The request sent by BT to A.N.A.F. will include the following data of the non-resident: name, surname, date and place of birth, gender, home address, data and copy of the identity document, tax identification code from the country of residence (if any). BT can also send to A.N.A.F. the proving documents of information submitted in the request. Based on the data submitted, the Ministry of Finance assigns the fiscal identification number or, as the case may be, the fiscal registration code, fiscally registers the respective person and communicates the information related to the fiscal registration to BT.

** O.N.P.C.S.B. - If the conditions are met for the transmission by BT of some personal data to the National Office for the Prevention and Combating of Money Laundering, according to the legislation for the prevention and combating of money laundering and the financing of terrorism, they are transmitted simultaneously and in the same format and to A.N.A.F.

*** C.R.C. - The bank has the legal obligation to report to the Credit Risk Register (C.R.C) within the B.N.R. credit risk information for each debtor that meets the condition to be reported (includes the identification data of a natural person debtor and operations in lei and in foreign currency through which the Bank exposes itself to the risk of that debtor) , respectively to have registered against him an individual risk, as well as the information about detected card frauds.

**** Biroul de Credit S.A./participants in the Credit Bureau system - the Bank has the legitimate interest to report in the Credit Bureau System, to which the other Participants also have access (mainly credit institutions and non-banking financial institutions, as joint controllers of the bank and the Credit Bureau) the personal data of the Customers who have contracted loans, as well - under certain conditions- of Customers who register delays in loan

payment of at least 30 days. The data is disclosed to these recipients also in the case of queries of this system, carried out by the bank in the process of analyzing a credit request or application.

IX. Transfers of Customer data to third countries or international organisations

Some of the contractual partners who provide us with services necessary for the proper performance of our activity and/or their subcontractors are not located in the European Union (E.U.) or in the European Economic Area (E.E.A), but in other states ("third countries").

When these partners/their subcontractors or international organizations may have access to the personal data that we process, we will only allow the transfer of data when strictly necessary and only on the basis of adequacy decisions or, in the absence of such decisions, based on appropriate safeguards provided by the GDPR.

To ensure that these transfers respect human rights, in particular the right to adequate protection of personal data wherever it is processed, we commit that - both before allowing the transfer of data to third countries or international organizations, and throughout the period in which the transfer is carried out, including when there are changes in the circumstances originally envisaged – we shall carry out assessments to see whether there are risks for the rights and freedoms of the data subjects and to manage those risks accordingly, including by taking necessary supplementary measures, so that the data benefit from the same level of protection they would have in the E.U./.E.E.A.

The European Commission may decide that some third countries, some territories or some sectors of a third country provide an adequate level of protection for personal data. The European Commission has issued adequacy decisions for the following third countries/sectors: Andorra, Argentina, Canada (companies only), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay, Japan, United Kingdom, South Korea. To these countries/sectors (unless a contrary decision is issued in respect of any of them), as well as to other countries to which the Commission will in the future recognize an adequate level of protection, transfers of personal data do not require special authorizations and are assimilated to disclosures of personal data to recipients from the E.U./S.E.E. states. The updated list of third countries to which an adequacy decision has been issued is the one mentioned on the website of the European Commission.

To any other third country or international organization we will transfer personal data only on the basis of adequate guarantees provided by the GDPR, usually those consisting of Standard Contractual Clauses approved by the European Commission which you can find here and, if these guarantees will not be sufficient, we will also take other supplementary measures for adequate data protection.

By way of exception, if BT Customers order through the bank transactions in which the beneficiaries are located in third countries that have not been recognized to provide an

adequate level of personal data's protection, the transfer of data to those countries is based on the following provisions of the GDPR: the transfer that it is necessary for the performance of a contract between the bank and the Customer or for the application of certain pre-contractual measures, adopted upon the Customer's request or, as the case may be, the transfer is necessary for the conclusion of a contract or for the performance of a contract concluded in the interest of the data subject.

X. Automated decision making, including profiling

In some circumstances, only in respect of GDPR provisions, in ouractivity we use automated decision-making processes, including as a result of profiling.

These are decisions taken by the bank based on automated processing of personal date, , with or without the intervention of a human factor, which can produce legal effects and/or affect the Customers in a similar way, to a significant extent.

Such situations are the following:

➢ for the application of the know your customer (KYC) measures in order to prevent and combat the money laundering and terrorist financing (including for the implementation of international sanctions), verifications will be carried out in the databases which include persons suspected of financing acts of terrorism, in lists of international sanctions orin warning lists with persons with a high risk of fraud. If the data subjects are included in these records, the bank reserves the right to refuse to enter into a business relationship with them or to terminate the contractual relationship or, upon case, to refuse the processing of the occasional transaction they initiated. For the same purpose, we will send and receive from D.G.E.P. data from the identity document of customers/ persons who go through the steps to become BT customers. We will record the data received from D.G.E.P. or, as the case may be, update it in our records as data from the customer's identity document. BT will not adopt any measure likely to produce legal effects or that would similarly affect customers to a significant extent solely on the basis of the automatic processing of data provided by D.G.E.P., unless the provisions of art. 22 of the General Data Protection Regulation (GDPR);

➢ to protect BT Customers and BT walk in clients against fraud, as well as for the bank to properly fulfill its KYC obligations, it monitors the Customers transactions and, if it identifies suspicious transactions (such as unusual payments as frequency, value, reported to the source of funds declared or the purpose and nature of the business relationship, transactions initiated from different cities at short time intervals, which did not allow the travelling between those cities, transactions whose details generate suspicions of money laundering or terrorist financing, attempts to use BT cards on suspicious websites), may take measures to block the transactions, accounts' cards, taking these decisions solely based on automatic processing;

➢ according to the legal provisions, the granting of the credit products is conditioned by the existence of a certain degree of indebtedness of the applicants. The eligibility to contract a credit product in relationship to the degree of indebtedness will be determined based on automated criteria, starting from the level of the income and expenses that the applicant Customer records;

➢ in order to objectively verify the fulfillment of the eligibility conditions for the pre-offer and, as the case may be, to analyze a credit application of an applicant- individual or legal entity to BT, in most cases, a scoring application of the bank will be used, which will analyze the data from the credit application, the information resulting from the verifications carried out in the bank's own records and/or those of the Credit Bureau S.A. and will issue a score that determines the credit risk and the probability of paying the installments in time. The result of other verifications of the applicant's status, will be added to the issued score, which will be analyzed by the bank's employees, to determine if the eligibility conditions established by the internal regulations, are met. The final decision to approve or reject the credit application is based on the analysis performed by the Bank's employees (human intervention). Exceptions to human intervention are in situations when you request credit products exclusively online. In these cases, we will take the decision to grant credit or, upon case, to reject the credit application based on solely automatic data processing. Taking the decision through such means is necessary in order to quickly analyze the request and conclude the credit agreement. However, you are guaranteed the right to request human intervention, meaning the analysis of the loan application by a bank employee, to express your point of view and to contest the solely automated decision;

➢to confirm your identity in the case of opening a remote business relationship, in the case of updating data by online means or for remote identification by video means, certain information of your face (taken from a still image or video) is compared with the picture from identity and, if you are already a BT Customer, the information extracted based on your face and from the identity document is compared with the ones we already have in the bank's records. Also, as part of these online processes, your access to your phone number, email address is checked and the contact data are also checked against those already declared to BT (if you are a BT Customer). If following these automated processes we identify inadvertences we will carry out checks through our employees and, if necessary, we will ask you to repeat the enrollment/update/identification process in a BT unit;

➢ if the BT Customers have expressed, on the dedicated form, their consent for the processing of personal data for marketing purposes, we shall create their profile based on different criteria (e.g. data on transactions, age, location, income range), which we will automatically study to assess what marketing messages would be relevant for them. In some cases, this profile will only have as consequences that only the Customers fulfilling the conditions of the profile will be sent certain marketing messages. In other cases it will determine that only the persons who fulfill the criteria of the profile will be able to contract/benefit from certain promotional offers. However, the rest of the Customers can benefit from the products/services under standard conditions.

XI. How long do we keep the personal data of Customers

1. Retention period for Customer data as a result of the request to establish/performance of a business relationship with the Bank or as a result of the request to use/the use of BT products/services

According to the legal obligation we have, the personal data we process for the application of know your customer (KYC) measures to prevent money laundering and terrorist financing, together with all the records obtained by applying these measures, such as monitoring and verifications carried out by the bank, documents supporting documents and records of transactions, including the results of any analysis carried out in relation to the Customer, which determines the Customer's risk profile, must be kept for **5 years after the termination of the Customers's business relationship** with the bank.

We are subject to the legal obligation to keep this data for the above mentioned period even if the Customer's request to open the business relationship with the bank is rejected or in case the Customer waives the request. In this case, the 5-year retention period will be calculated from the date of rejection of the request or the Customer's withdrawal, respectively from the date of the occasional transaction.

At the request of the competent authorities, the initial legal period of 5 years mentioned above **may be extended, up to a maximum of 10 years after the termination of the business relationship**.

At the expiration of the legal retention period (initial or extended, upon case), the bank will delete or anonymize this data, except in cases where other legal provisions require their longer retention. Other legal provisions that oblige us to keep Customer data for longer periods are those of:

- the Fiscal Procedure Code, which provides that part of the data processed for the application of KYC measures must also be processed for reporting to A.N.A.F. The legal retention period for this data is **10 years from the termination of the business relationship or from the occasional transaction date;**

- the financial and accounting legislation provides that the relevant accounting documents for the financial records and the supporting documents, including the contracts based on which the accounting entries were made (implicitly the personal data contained in them) must be kept for up to **10 years from the end of the financial year in which they were created;**

- the national legislation applicable in the field of electronic signature obliges the suppliers who issue digital certificates to keep the information regarding a qualified certificate for a period of **at least 10 years from the date of its expiry**. In cases where the Romanian providers we collaborate with in this field process personal data as joint controllers with the bank, we may need to keep the data regarding the certificates for this period;

- for the Customers whose personal data were queried in the A.N.A.F. records (according to the consent they expressed), the legal term imposed for keeping the query consent forms (by default also for the personal data contained therein) is **8 years;**

As for the data that the bank has the legal obligation to report to the Credit Risk Register (C.R.C.), the documents containing the credit risk information and the information about the reported card frauds (including the personal data from them) are kept for a period of **7 years**.

Regarding the data processed in the Credit Bureau system based on the legitimate interest of the Participants in this system, they are stored at the level of this institution and disclosed to the Participants for **4 years from the date of the last update**, with the exception of the data of credit applicants who have abandoned their application of credit or whose application was rejected, which are stored and disclosed to Participants for a period of **6 months**.

For all cases where your data is subject to more than one retention period, the longest of these will apply. After the longest term, the data will be deleted or anonymized.

2. Retention period for Customer data captured by video surveillance cameras

If you visit the bank's units (including office buildings) or BT equipment (ATMs, automated payment machines), your image is captured by the video surveillance system. The data collected by video surveillance cameras are kept for 30 days, after which they are automatically deleted. In well-justified specific cases, only in compliance with the applicable legal provisions, the retention period of the relevant video recordings can be extended up to 6 months from the end of the month in which the images were recorded or, if necessary, for a longer period, up to completion of investigations of the incident that led to the extension of the storage period. In the case of video images that are the subject of access requests to data, the retention periods for BT petitioners' personal data apply.

3. Retention period for the data of Customers who have expressed their choices for marketing

The data of BT Customers who have expressed their consent to receive marketing messages are processed for this purpose until the consent is withdrawn or, otherwise, until the termination of their quality as a BT Customer.

4. Data retention period of data belonging to Customers who have addressed petitions to the bank (Customers -BT Petitioner)s

In order to prove that we have received from you notifications/complaints/requests for information/measures and that responses to them have been formulated and sent, the data related to these petitions will be kept (together with the personal data contained therein) in the case of BT customers for the duration of their business relationship with the bank to which 3 years are added (legal prescription period).

Any other personal data processed by BT for other purposes indicated in this privacy notice will be kept for the period necessary to fulfill the purposes for which they were collected, to which non-excessive terms may be added, established according to the applicable legal obligations in the field, including but not limited to to the provisions on archiving, or established internally, according to the legitimate interests of the bank.

XII. Rights of BT customers in regard to the processing of their personal data

All BT Customers are guaranteed the rights below regarding their personal data processed by BT.

You should know that we treat these requests with the highest degree of professionalism and their situation is periodically brought to the attention of the Bank's management.

Each of the requests is carefully analyzed, the responses to the requests are documented and, whenever necessary, we take corrective measures to ensure that we respect the rights you have regarding the legal processing and proper protection of your data, which is an essential component of our obligation to respect human rights.

a) right of access: the Customers can obtain from BT the confirmation that their personal data are processed, as well as information regarding the reasoning of the processing such as: purpose, categories of personal data processed, data recipients, period for which the data are kept, the existence of the right of rectification, erasure or restriction of the processing. This right allows the data subjects to obtain for free a copy of the personal data processed;

b) right to rectification: the Customers can request BT to modify the incorrect data concerning them or, as the case may be, to complete the data which are incomplete;

c) right to erasure (right "to be forgotten"): the Customers may request the deletion of their personal data when:

• these are no longer necessary for the purposes for which the bank collected and processed them;

• the consent for the processing of the personal data has been withdrawn and BT can no longer process it on the basis of other grounds;

• the personal data are processed against the law;

• the personal data must be deleted in accordance with the relevant legislation;

d) withdrawal of consent: the Customers may withdraw their consent at any time regarding the processing of personal data processed on this legal ground. Withdrawal of consent does not affect the lawfulness of the processing carried out before the withdrawal;

To withdraw consent for data processing for marketing purposes, you can also use the following online form available in the **Privacy Hub** section „Do you want marketing or not?" (options for BT customers) and check the option "I do not want to receive marketing messages"/"nu doresc mesaje publicitare";

e) right to object: the Customers can, at any time, object to the processing for marketing purposes, as well as to processing based on the legitimate interest of BT, for reasons related to their specific situation;

f) right to restriction of processing: the Customers may request the restriction of processing of their personal data if they:

• dispute the accuracy of the personal data, for a period that allows the bank to verify the accuracy of the data in question;

• the processing is illegal and the Customer opposes the erasure of the personal data, requesting instead the restriction of their use;

• the data are no longer necessary to us, but the Customer asks for them for an action in court;

• if the Customer has opposed to the processing, for the period of time in which we verify whether the legitimate rights of BT as a controller prevail over the data subject's rights.

g) right to portability: the Customers may request, according to the law, the bank to provide certain personal data in a structured form, commonly used and machine-readable format. If the Customers request, BT may transmit the respective data to another entity, if this is technically possible.

h) rights regarding solely automated decision-making: as a rule, Customers have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects on them or similarly significantly affects them. They have the right to express their point of view, to contest the decision and to request human intervention (review of the automated decision by a BT employee).

h) the right to file a complaint with the National Supervisory Authority for the Processing of Personal Data: Customers have the right to file a complain with the National Supervisory Authority for the Processing of Personal Data if they consider that their rights have been violated:

National Supervisory Authority for the Processing of Personal Data, B-dul G-ral. Gheorghe Magheru 28-30, Sector 1, postal code 010336, Bucharest, România, e-mail: anspdcp@dataprotection.ro.

To exercise any of the rights mentioned in points a) - h) above at BT, the data subjects should use the contact details of the data protection officer designated by BT (BT DPO), by sending the request in any of the below mentioned methods:

- at the e-mail address dpo@btrl.ro

- by filling in the online form available for Customers from the section: "How to exercise your GDPR rights at BT" available on **Privacy Hub**

- by mail, at the following address: Cluj-Napoca, str. Calea Dorobanților, no. 30-36, Cluj County, with the mention "in the attention of the data protection officer"

Before sending us your request, we recommend that you read the instructions in the "How to exercise your GDPR rights at BT" section available in the **Privacy Hub**.