TÜRKİYE GARANTİ BANKASI A.Ş.

PERSONAL DATA PROTECTION AND PROCESSING POLICY

September 2020

Version 1

LIST OF INDEX

1-SCOPE AND PURPOSE

2-DEFINITIONS

3-SOURCES

4-GENERAL PRINCIPLES ON PROCESSING OF PERSONAL DATA

5-PROCESSED PERSONAL DATA

6-PURPOSES OF PROCESSING OF PERSONAL DATA

7-TRANSFER OF PERSONAL DATA AT HOME OR ABROAD

8-PERIODS OF PROCESSING OF PERSONAL DATA

9-TECHNICAL AND ADMINISTRATIVE MEASURES TO BE TAKEN FOR SECURITY OF PERSONAL DATA

10-TRAININGS

11-PERSONAL DATA OF SPECIAL CHARACTER AND THEIR SECURITY

12-RIGHTS OF RELEVANT NATURAL PERSONS

13-DESTRUCTION OF PERSONAL DATA

14-SANCTIONS

1-SCOPE AND PURPOSE

We, as T. Garanti Bankası A.Ş., ("Bank") are showing respect to and care for privacy and confidentiality rights of our clients, employees, suppliers, providers and all other people.

That is why this policy document (the "Policy") regulating the rules followed and the norms and principles adopted in reliance upon the Personal Data Protection Law no. 6698 (the "Law") put into force with a view to protecting your fundamental rights and freedoms, in respect of processing, use and protection of personal data acquired in the course of all kinds of banking activities and operations carried out by our Bank in strict compliance with all applicable laws and regulations, particularly the Banking Law, governing our Bank, has been prepared and issued, and as said, this Policy sets down the rules and principles required to be abided by our Bank with regard to personal data. This Policy is applicable primarily in our country where our Bank is active and operating, and also in other country where our Bank has banking operations and activities, to the extent permitted and allowed by the pertinent laws and regulations of the relevant country. Furthermore, the general principles set down in this document should be accepted as valid and applicable on the part of our affiliates as well. This means to say that our affiliates are expected to formulate their own policies in connection herewith parallel to the principles of this Policy.

The actions and measures which are not mentioned in this Policy document because of being characterized as Bank secrets and not disclosed to public therefor, and particularly, the actions and measures for security of personal data, as well as more detailed rules and provisions aimed at implementation of this Policy are set down in sub-procedures and processes, and in the Bank's internal circulars, notifications and memoranda.

All employees of T. Garanti Bankası A.Ş. and its affiliates are, if they process any personal data in the course of their business activities and operations, obligated to comply with the general law norms, and the Law, and the rules set down in this Policy document.

The information note published by our Bank as a requirement of its public disclosure obligations arising out of article 10 of the Law may be retrieved by clicking here.

Our Bank further applies policies and procedures in respect of data security and sharing rules.

All principles and applications regulated and adopted in this Policy document are being supported by other documents referred to in the preceding paragraph.

2-DEFINITIONS

For the purposes and in the context of this Agreement:

“Banking Law” refers to the Banking Law no. 5411, and

“Bank” refers to and stands for Türkiye Garanti Bankası A.Ş., and

“BRSA” refers to and stands for Banking Regulation and Supervision Authority, and

“Related Person” refers in general to all natural persons whose personal data are processed by our Bank, including, but not limited to, our clients, prospective clients, employees, candidate employees, relatives and friends of employees, trainees, candidate trainees, shareholders, visitors, suppliers and providers, employees of suppliers and providers, employees of affiliates, other persons or entities entering into collaboration with our Bank, and natural persons or employees authorized to represent the legal entities having business relations with our Bank, and

“Law” refers to and stands for the Personal Data Protection Law no. 6698 published in the Official Gazette edition 29677 on 7.4.2016, and

“Personal Data” refers to all kinds of information about an identified or identifiable natural person, and

“Processing of Personal Data” refers to all kinds of operations conducted on data, such as acquisition, registration, recording, storage, safekeeping, modification, rearrangement, disclosure, transfer, receipt, making available, classification or prevention of use of Personal Data either by entirely or partially automatic ways or means or by non-automatic ways or means, providing that they are a part of any data registration system, and

“KVK Authority” refers to and stands for the Personal Data Protection Authority, and

“KVK Board” refers to and stands for the Personal Data Protection Board, and

“Destruction Policy” refers to Personal Data Storage and Destruction Policy of T. Garanti Bankası A.Ş., and

“Personal Data of Special Character” refers to data regarding race, ethnical origin, political thought, philosophical belief, religion, sect or other beliefs, attire, membership in associations, foundations or unions, health, sexual life or orientation, criminal conviction records and security measures of individuals, as well as their biometrical and genetic data, and

“Data Supervisor” refers to a natural person or a legal entity which is in charge of determination of processing purposes and means of personal data, and installation and management of data registration system. Our Bank, as a separate legal entity, is a data supervisor.

3-SOURCES

This Policy is based and relied upon the Constitution, the Law, the Banking Law, all and any regulations issued by BRSA in reliance upon the Banking Law, and regulations, communiqués, guidelines and good practices manuals published by the Personal Data Protection Authority in reliance upon the Law, GarantiBBVA Code of Conduct, as well as our Bank's internal circulars, policies, processes, memoranda and notifications.

4-GENERAL PRINCIPLES ON PROCESSING OF PERSONAL DATA

As per the Law, our Bank, as a separate legal entity, is a data supervisor.

Our Bank is processing the personal data of the related persons in accordance with the following general principles, pursuant to 2nd paragraph of article 4 of the Law and for the objectives and purposes declared in Part 6 of this document:

- Compliance with the law and the good faith rules, and
- Being true, accurate and if needed, current and updated, and
- Being processed for particular, clear and legitimate purposes, and
- Being interconnected to, limited by, and proportionate to, the purposes of processing, and
- Being kept only for a period of time foreseen in the relevant legislative instruments or required for the purposes of processing.

Our Bank is also acting in compliance with other fundamental principles set forth in the Constitution and in other laws and regulations for the sake of protection of fundamental rights and freedoms of the related persons, without limiting itself by these principles.

5-PROCESSED PERSONAL DATA

Personal data which differ by the type, nature and history of relations between our Bank and the related person, and by the method of acquisition of data, and by the purposes set down in article 6 of this Policy, and which are processed in conformity with the principles regulated by this document, generally include, but are not limited to, the following items:

- Various different demographical data introducing the data subject, such as first name, surname, profession, job title, employment information, education status, gender, marital status, spouse/children data, curriculum vitae data, citizenship status, nationality, tax liability status and other information relating directly to the person, and
- Images or photos of documents used for identification purposes, such as identity document, professional identity document, passport and driver's license, and such data as date of birth, place of birth, identity number, public

registration data, blood group, religion, photograph and professional data that may be given on such identity documents, and

- Client information, IP addresses, passwords and code numbers needed to enter into electronic banking channels, and position data processed for performance of security applications and satisfaction of legal obligations used in said channels, as well as biometrical data processed in reliance upon a prior consent of the related person, and
- Communication data and information such as address, electronic mail address, registered electronic mail address, mobile phone, fixed phone and facsimile number, together with communication records of phone calls and conversations, video conversations and electronic mail correspondences, and other audio and visual data and information, and
- Data and information of natural persons in documents used for identification of legal entities such as tax chart, trade registry gazette, certificate of authorization, trade registry documents, certificates of competence, signature circular and activity certificate, and
- All kinds of detailed financial data and information relating to pricing, account reconciliation and client data and information produced by our Bank, and uniform numbers of products and services received by clients from our Bank, and credit reference numbers, credit card numbers, account numbers, IBAN, collection and payment activities and operations, and
- Payroll information, disciplinary investigations, recruitment and dismissal data and records, declarations of properties, curriculum vitae data, performance assessment reports, diploma data, courses attended, on-the-job training data and information, certificates, academic transcripts and similar other personal data and curriculam vitae of employees and potential employees, and
- Such data as information in correspondences with juridical authorities, information in case files, and information kept in respect of alternative ways of resolution of disputes in the course of legal disputes and proceedings involved in by our Bank, and
- Data contained in letters of all and any administrative and juridical authorities and bodies communicated to our Bank, and
- Such data as records and camera views of entrance and exit of employees and visitors kept for the sake of physical security in locations belonging to our Bank and its affiliates, and
- Data required for monitoring, reporting and control of consolidated risks of our Bank and its affiliates arising out of or in connection with the applicable laws and regulations, and
- Data such as shopping history, public surveys and questionnaires, cookie records, and results of campaigns that may be kept in line with consents received from our clients and prospective clients and other natural persons related to them.

6-PURPOSES OF PROCESSING OF PERSONAL DATA

Purposes of processing of personal data by our Bank vary according to the specific activities and operations of our Bank, but nevertheless they include, but are not limited to, the following purposes:

- To present and offer via all channels, also including electronic banking channels, all of our products and services, particularly deposit, crediting, payment services, insurance, individual retirement and investment services, which are offered by our Bank as an agency or are mediated by our Bank, pursuant to the Banking Law and all other applicable laws and regulations pertaining thereto; and
- To register and record identity, address and other required data in order to identify our clients before or in the course of their banking transactions; and
- To transmit via communication data all and any important and material data and information required to be shared by our Bank with the relevant natural persons; and
- To regulate all of the required records and documents, also including the processing of position data, for the sake of completion of banking transactions on paper and in verbal media and electronic banking media (internet banking, mobile banking, ATM and telephone banking); and
- To keep, store, and report all and any information that may be requested by such public or regulatory authorities such as BRSA, TCMB (Turkish Central Bank), MASAK (Financial Crimes Investigation Board), GIB (National Revenues Department), CMB (Capital Markets Board) and TBB (Bankers Association of Turkey) Risk Centre, and to keep these authorities informed; and
- If to use such personal data for presentation and offering of our products and services which are covered by and in respect to the applicable laws and regulations particularly the Personal Data Protection Law, and to plan and implement product, service and offering activities specifically for our clients, for the purposes of improving, updating, and renewing banking products and services with developing technology, to prepare product, service and working model offers, to conduct profiling and segmentation works, to formulate and create our Bank's internal targets, to make scoring and risk analyses, to manage client relations, to use the same in our Bank's internal performance assessments and analyses, to design our Bank's servicing models through statistical works, and to carry out market studies and researches; protect our customers, our Bank and the Banking System against fraud and attacks they may be exposed to in any physical or electronic environment; and
- To record camera views in our branches, regional directorates and head offices buildings due to the premises security applications; and
- To plan, supervise, audit and implement our corporate sustainability, corporate governance, strategic planning and information security processes; and
- To fulfil our administrative and legal obligations and the requirements of our contracts and agreements signed with all related parties.

Specifically for our employees, candidate employees, trainees and candidate trainees:

- To manage and handle business relations with our Bank; and
- To share personal data with, and transfer the same to the Bank and its main shareholder seated abroad, and its local and foreign subsidiaries, and to fulfil all legal obligations in connection therewith, in accordance with the purposes of such relations; and
- To complete the registrations, notifications and applications regarding all kinds of personal data of special character, particularly biometrical data, pursuant to the Labour Act no. 4857, the Social Securities and Public Health Insurance Law no. 5510, the Worker's Health and Job Safety Law no. 6331 and other pertinent laws and regulations; and
- With a view to keeping and storing the records and documents for the periods of time specified in the applicable laws, and fulfilling the data storage, reporting and information obligations arising out of the applicable laws, and enforcing the provisions of all contracts entered into by our Bank, also including private health insurance, to process personal data for disclosing to and sharing with the Ministry of Justice, the Interior Ministry, the Ministry of Family, Labour and Social Services, the Social Security Authority, the Turkish Employment Agency and such other public authorities and institutions and the Ministry of Treasury and Finance of the Republic of Turkey, and such public and/or private law legal entities as T. Garanti Bankası A.Ş. Officers and Servants Social Aid and Pension Fund and notaries public, and all and any persons or entities permitted by the Banking Law and all other applicable laws and regulations, and financial institutions listed in article 73/4 of the Banking Law, and public legal entities such as BRSA, CMB, TCMB, SPL (Capital Markets Licensing), and Insurance Supervision Centre, and our Bank's main shareholder, direct / indirect local / foreign subsidiaries, and its program partners which provide services to or enter into collaboration with our Bank in the course of conduct of its banking activities and operations, and the contracted Joint Health and Security Units (GSGB) and other third parties, including, but not limited to, inhouse doctors and job safety specialists.
- Monitoring compliance with the laws, published policies, standards that the Bank is subject to in physical and electronic environment, making quality and compliance measurements and investigating cases, investigations, misconduct, etc.

7-TRANSFER OF PERSONAL DATA AT HOME OR ABROAD

Our Bank shares personal data with other persons and entities only for the purposes permitted by the Law, by also taking into consideration the secrecy and confidentiality obligations, to the extent permitted by the Banking Law and in particularly considering provisions of the Personal Data Protection Law.

The exceptions thereto may be listed as follows:

- Exchange and all kinds of information and documents by and between banks and financial institutions either directly among themselves or indirectly through risk centre or through companies to be founded by at least five banks or financial institutions, providing, however, that a confidentiality contract is

signed therebetween, and only the purposes cited hereinabove are pursued thereunder; and

- Assessment and appraisal works to be conducted by prospective buyers for the purpose of sale of shares representing ten percent or more of share capital of banks through direct or indirect shareholdings; and
- (i) Preparation of consolidated financial statements, (ii) risk management and (iii) internal audit applications of main partners or shareholders holding ten percent or more of share capital of the Bank, including, but not limited to, crediting institutions and financial institutions resident at home or abroad; and
- Assessment and appraisal works to be conducted for sale of assets, also including credit facilities, of our Bank or of securities relied upon them; and
- Assessment and valuation works; and
- Rating works; and
- Outsourcing of support services; and
- Independent audit activities; and
- Use in transactions for outsourcing of services, providing that all actions and measures are taken for the sake of security of data, information and documents.

Within the frame of article 73/3 of the Banking Law, data of natural persons or legal entities acquired in the course of or after establishment of a client relationship with banks in respect of banking activities and operations become a client secret. Without prejudice to the mandatory provisions of other laws and regulations, information characterized as client secrets are not shared with or disclosed to third parties at home or abroad, without a specific demand or instruction of the client, even in presence of an explicit prior consent of the client, pursuant to the Law, save for the exceptions of secrecy and confidentiality obligations dealt with in article 73/4 of the Banking Law.

As a consequence of an assessment of economic security, BRSA is authorized to prohibit the sharing of all kinds of data characterized as client secrets or bank secrets with third parties seated abroad, or disclosure of such data to them, and also to take decisions on keeping at home of the information systems used by banks in conduct and performance of their banking activities and of the backup and standby systems.

Also including the disclosure of data in cases of exceptions from the secrecy and confidentiality obligations set down in fourth paragraph of article 73 of the Banking Law, the data and information characterized as client secrets and bank secrets may be shared and disclosed **only for the purposes specified therefor,** providing that they cover and contain only data required for said purposes, **in accordance with the principle of proportionateness.**

BRSA is authorized to determine the scope, format, procedures and principles of disclosure and transfer of secret data and information pursuant to third and fourth paragraphs of article 73 of the Banking Law, or to put limitations or restrictions thereon.

Pursuant to the Law, personal data and personal data of special character may be transferred at home or abroad in reliance upon an explicit consent of the related person and/or for the legal reasons set down in second paragraph of article 5 of the Law and again for the purposes and under the conditions stated in third paragraph of article 6 of the Law, providing that all kinds of measures adequate for assuring security of data are properly taken therefor.

8-PERIODS OF PROCESSING OF PERSONAL DATA

In determination of the periods of storage and destruction, the Bank will take into consideration the periods of time stated in article 42 of the Banking Law, and in provisions of the Regulation of BRSA on Procedures and Principles on Storage of Documents and on Accounting Applications of Banks, and in other applicable laws and regulations, as well as the periods of time specified in its Destruction Policy and in its Personal Data Processing Inventory on the basis of its activities and operations.

Storage Time	**Legal Grounds**
10 (ten) years	Article 42 of the Banking Law no. 5411, and Article 17 of Regulation on Procedures and Principles on Storage of Documents and on Accounting Applications of Banks

9-TECHNICAL AND ADMINISTRATIVE MEASURES TO BE TAKEN FOR SECURITY OF PERSONAL DATA

Our Bank takes, and is under obligation to take, all kinds of technical and administrative measures so as to assure the desired level of security appropriate for the purposes of

- Prevention of illegal and unlawful processing, and
- Prevention of illegal and unlawful access, and
- Assurance of storage and safekeeping

of personal data acquired and processed in the course of its banking activities. In taking these measures, our Bank relies upon all primary and secondary legislative instruments applicable on our Bank, particularly BRSA's Regulation on Information Systems and Electronic Banking Activities of Bank and the Personal Data Protection Authority's Guideline on Security of Personal Data (Technical and Administrative Measures), as well as the sources listed in part 3 of this Policy document.

In addition, Garanti BBVA Code of Conduct and Integrity; reminds that the data belonging to customers, employees and any third party that employees access during their professional activities are confidential, and that measures for the acquisition,

storage and access of this information should be followed and comply with the relevant procedures.

10-TRAININGS

After the effective date of the Law, training activities aimed at increase of awareness on the Law are organized for all employees of our Bank and its affiliates, and all of the employees are ensured to take these training events mandatorily. Training contents are regularly updated, and trainings are assigned to both newly recruited employees and the existing employees.

11-PERSONAL DATA OF SPECIAL CHARACTER AND THEIR SECURITY

Article 6 of the Law defines data regarding race, ethnical origin, political thought, philosophical belief, religion, sect or other beliefs, attire, membership in associations, foundations or unions, health, sexual life or orientation, criminal conviction records and security measures of individuals, as well as their biometrical and genetic data, as personal data of special character.

The processing of such personal data of special character without an explicit consent of the relevant natural person is prohibited. Exceptions of this are:

- Personal data, other than health and sexual life or orientation, may be processed only in specific cases foreseen in the laws, without an explicit consent of the related person (race, ethnical origin, political thought, philosophical belief, religion, sect or other beliefs, attire, membership in associations, foundations or unions).

- Personal data relating to health and sexual life and orientation may be processed only for protection of public health, and conduct of protective medicine, medical diagnosis, treatment and care services, and planning and management of healthcare services and financing, only by persons or authorized entities and institutions under secrecy and confidentiality obligations, without an explicit consent of the related person.

Adequate measures required to be taken in the processing of personal data of special character are determined as listed above by a Decision no. 2018/10 dated 31.1.2018 of the Personal Data Protection Board. According to this decision, actions needed for the listed measures are taken in the Bank by also taking into consideration the technical and administrative measures for achievement of an appropriate level of security as stated in the Personal Data Security Guideline published in the internet site of the Personal Data Protection Authority.

12-RIGHTS OF RELEVANT NATURAL PERSONS

The related natural persons may apply to our Bank and may:

- Learn whether their personal data are processed or not, and if processed, learn the purposes of processing, and whether they are used for the intended purposes or not, and if processed, request information thereabout; and
- Learn third parties with whom their data and information are shared at home or abroad in accordance with the Law; and
- If they think or believe that their personal data are processed deficiently or inaccurately, may request correction or completion of the same; and
- Request deletion or destruction of their personal data within the frame of the terms and conditions stipulated in article 7 of the Law; and
- Request that their demands stated in paragraphs (c) and (d) are notified also to third party receivers of their personal data, and that the same actions are taken also by said third party receivers; and
- Raise an objection against any consequences that may be in disfavour of them due to analysis of their personal data by automatic systems, or if they believe that their personal data are recorded or used unlawfully, and they have suffered damages due to that reason, they may claim indemnification of their damages and losses.

If applications made for these purposes require an additional cost, the amount of fee shown in the tariff rates to be determined by the Personal Data Protection Board may be required to be paid. Your demands included in your application will be responded and finalized as soon as possible and in any case within no later than 30 (thirty) days at the latest, depending on the nature of demand.

In order to use your rights arising out of the Law, you may file your applications in writing, via registered electronic mail (KEP) address, by secure electronic signature, mobile signature, or via your electronic mail address previously designated to our Bank and registered in our Bank's system, and in order to get detailed information and to receive more detailed information about the method of use of the rights of objection against the reply given by our Bank, you may visit the internet page of the Personal Data Protection Authority.

13-DESTRUCTION OF PERSONAL DATA

In order to determine the principles required to be complied with insude the Bank and/or by the Bank and to be applied in deletion, destruction or anonymization of personal data contained in the Regulation on Deletion, Destruction or Anonymization of Personal Data issued pursuant to article 7 of the Law and published by the Personal Data Protection Authority on 28.10.2017, and for the sake of ensuring compliance with the provisions of the Regulation, our Bank's Personal Data Storage and Destruction Policy is prepared, issued and put into effect as of 1.1.2018.

If and when new legislative instruments are enacted in connection therewith, or the relevant existing legislative instruments are updated, our Bank will comply with the requirements of all legislative instruments by updating its Destruction Policy in accordance with the pertinent applicable laws and regulations.

If and when it is believed that there is a legal barrier in implementation of this Destruction Policy by the Bank, then and in this case, our Bank will redetermine and

rearrange the steps to be taken in due consultation with the Personal Data Protection Authority in case of need.

BRSA's Information Systems Management and Electronic Banking Regulation provisions are also included in the scope of the Destruction Policy.

By its Destruction Policy, our Bank accepts to cover all personal data kept in the following data registration media, as well as all other additional media that may be developed in the future.

a. Computers / servers / databases used in the name of the Bank,

b. Network devices,

c. Shared/unshared disk drivers used for storage of data on network,

d. Cloud systems,

e. Mobile devices and all storage areas inside them,

f. Paper,

g. Micro fiche,

h. Peripheral devices such as Printer, Fingerprint reader,

i. Magnetic bands,

j. Optic disks, and

k. Flash memories.

Personal data may be destroyed by three different methods, namely deletion, destruction or anonymization of data. The purpose underlying the destruction is to prevent the identification of natural person by using the remaining data.

Unless otherwise decided by the Personal Data Protection Board, the Bank ex officio chooses appropriate one of the methods of deletion, destruction or anonymization of personal data. Upon demand of the related data subject, the Bank chooses the appropriate method by also justifying its choice. The Bank will separately act in line with BRSA's Regulations on Information Systems and Banking Processes in relation therewith.

All actions taken by our Bank in respect of deletion, destruction or anonymization of personal data are recorded and registered, and said records are kept for at least 3 (three) years, except for other legal obligations.

Periodical destruction is conducted in our Bank in 6 (six) months' time intervals.

(i) Deletion of Personal Data

Data will be deleted if and when the Bank processes the personal data entirely or partially by automatic means, and in case of deletion of personal data, the Bank makes the data inaccessible or non-reusable by the related users in any cases or events. In taking these actions, the Bank must guarantee that the personal data

become inaccessible or non-reusable by the related users. This guarantee is under responsibility of the data supervisor.

If, during deletion, the personal data which should not be deleted due to legal causes or reasons are also affected from the deletion and become inaccessible and/or non-reusable, then, the Bank's related units and divisions may take the required decisions and implement the following methods all together, which will also be considered and treated as deletion:

a) Archiving of personal data in such manner to ensure that they can no more be associated with the related person, and
b) Keeping of personal data closed to all kinds of accesses, and
c) All kinds of technical and administrative measures required to be taken as per BRSA's Regulations on Information Systems and Banking Processes in such manner to ensure that they are accessible only by authorized persons and only if and when needed absolutely.

(ii) Destruction of Personal Data

Destruction means to make personal data inaccessible and non-reusable by anybody in any manner whatsoever. The Bank takes all kinds of technical and administrative measures required for destruction of personal data.

(iii) Anonymization of Personal Data

Anonymization means to make personal data unassociable with any identified or identifiable natural person in any manner whatsoever even if they are matched to other data and information.

During anonymization of personal data, the Bank uses technical methods which guarantee irreversibility. Furthermore, in choice of these methods, the regulations and guidelines published by the Personal Data Protection Authority may also be used.

14-SANCTIONS

I- Crimes

Crimes relating to personal data, and penal sanctions applicable on crimes are regulated in the related provisions of the Turkish Criminal Code no. 5237. Articles 135 to 140 of the Turkish Criminal Code regulate the crimes of unlawful or illegal registration of personal data, unlawful or illegal disclosure and acquisition of personal data, non-destruction of data, as well as the qualified forms of these crimes, together with administrative fines and punishments restricting personal freedom to be applied on these crimes.

II- Misdemeanors

The Law further describes the misdemeanors that may be exposed by data supervisor in case of breach of the obligations and liabilities of data supervisor, together with administrative fines to be applied on such misdemeanors. Accordingly, failure to perform public disclosure obligations, failure to ensure data security, failure in performance of the Board decisions, and violation of the obligations of registration in and notification to the Registry are considered as misdemeanors, and are made subject to administrative fine sanctions.

This Policy document has been prepared by T.Garanti Bankası A.Ş. and It was approved by the Board of Directors on September 3, 2020 and entered into force.