1. FOREWORD

Dear Valued Customers,

As IBS Sigorta ve Reasürans Brokerliği A.Ş. (IBS), we meticulously safeguard the information of our valued customers and anyone who has shared any personal data with us through any form of interaction. We have taken all necessary internal measures to ensure the security of this information. You may confidently conduct transactions with IBS Insurance and Reinsurance Brokerage Inc., knowing that your personal data is secure.

We respect your rights regarding your data, which are protected under the Constitution of the Republic of Türkiye and applicable laws. Below, we present our Data Protection Policy implemented within our company.

You can be assured that we will respond with full sensitivity to your suggestions for improvement, applications, and possible complaints. As IBS, you may contact us regarding any concerns about your personal data. Just as in all our services, we will show the same level of care and diligence in protecting your personal data.

Sincerely,

"If a printed copy of this document does not bear the 'CONTROLLED COPY' stamp, it is considered an uncontrolled working copy; the current version is maintained electronically."

2. INTRODUCTION

2.1. Purpose of the Policy

The protection of personal data is among the top priorities of IBS Sigorta ve Reasürans Brokerliği A.Ş. ("IBS" or "Company"), and we make every effort to comply with all applicable legislation.

Due to the sensitive nature of our business, all data obtained from policyholders or prospective customers has been kept confidential and has never been shared with third parties outside of insurance operations. Protecting personal data has always been a fundamental principle of our company, even before legal regulations were introduced.

Within the framework of this Policy, the principles adopted in carrying out personal data processing activities and ensuring compliance with Law No. 6698 on the Protection of Personal Data ("Law") are explained. Thus, our Company ensures transparency by informing data subjects.

With full awareness of our responsibility, your personal data is processed and protected within the scope of this Policy.

2.2. Scope and Revision of the Policy

This Policy applies to all personal data processed partially or fully automatically or as part of a data recording system, excluding company employees, including:

- Individual customers
- Employees of corporate customers
- Other insured persons
- Job applicants

Detailed information about data subjects can be found in **Annex 1 – Data Subjects**.

2.3. Enforcement of the Policy

This Policy has been prepared in accordance with Law No. 6698 (KVKK). The Law has entered into force in full upon publication.

The Company reserves the right to amend this Policy. Any changes will be indicated with date and version updates.

This Policy is published on the Company's website and made accessible upon request.

"If a printed copy of this document does not bear the 'CONTROLLED COPY' stamp, it is considered an uncontrolled working copy; the current version is maintained electronically."

2.4. Authority and Responsibility

The Company, in its capacity as the Data Controller, is responsible for the implementation of this Policy in terms of its operation and the regulation of related processes.

All employees, business partners, visitors, and all relevant third parties across the Company are obliged to comply with this Policy and to cooperate with IBS in preventing any legal liabilities, risks, and potential hazards that may arise in accordance with applicable legislation.

This Policy is published on the Company's website. Any amendments to the Policy are updated on the website, thereby ensuring that data subjects are informed and have access to the principles set forth herein.

In the event of any inconsistency between this Policy and the applicable legislation in force, the Company, in its capacity as Data Controller, acknowledges that the provisions of the applicable legislation shall prevail.

3. PRINCIPLES REGARDING THE PROCESSING OF PERSONAL DATA

Within the scope of Law No. 6698, IBS acts as a **Data Controller** and processes personal data in accordance with the Constitution and applicable legislation.

Within the scope of the Law No. 6698 on the Protection of Personal Data ("KVK Law"), IBS, acting as the "data controller," complies with the general principles and conditions stipulated in the legislation regarding the protection and processing of personal data and acts in accordance with the following principles to ensure that personal data is processed in compliance with the Constitution and the KVK Law.

3.1. Processing in Compliance with Principles

IBS processes personal data in accordance with the following principles:

3.1.1. Lawfulness and Fairness

In accordance with Article 4 of the Law No. 6698 on the Protection of Personal Data, IBS processes personal data in compliance with the law and the principle of good faith, adopts the principle of transparency towards data subjects, and duly informs them.

"If a printed copy of this document does not bear the 'CONTROLLED COPY' stamp, it is considered an uncontrolled working copy; the current version is maintained electronically."

In such disclosures, clarity and honesty are essential; clear information is provided regarding the purposes for which personal data is collected, and the data is processed accordingly. It is fundamental that personal data shall not be used in a manner that would adversely affect the data subject without any legal justification.

3.1.2. Accuracy and Up-to-date

IBS ensures that the personal data it processes is accurate and up to date. Throughout the processing period, the Company takes all necessary measures, to the extent permitted by technical means, to maintain the accuracy and currency of personal data, and establishes the required administrative and technical mechanisms to periodically ensure such accuracy and currency.

3.1.3. Specific, Explicit, and Legitimate Purposes

Personal data is processed by IBS in a lawful manner, limited to the requirements of the applicable legislation and the services provided or to be provided. The purposes of processing are clearly and explicitly determined prior to the commencement of processing activities.

The Company collects and processes personal data lawfully and for legitimate purposes, and processes such data only to the extent necessary and in connection with its business activities.

3.1.4. Proportionality

Personal data is processed by IBS in a manner that is relevant, limited, and proportionate to the purposes for which it is processed. Accordingly, the Company avoids processing personal data that is unrelated to or unnecessary for the specified purposes. In this context, the principle of data minimization is adopted.

3.1.5. Retention Period

IBS retains personal data only for the period stipulated by the relevant legislation or required for the purpose of processing.

In this regard, it is first determined whether a specific retention period is prescribed under applicable legislation. If such a period exists, compliance with that period is ensured. If no specific period is stipulated, the data is retained for the duration necessary to fulfill the purpose of processing.

"If a printed copy of this document does not bear the 'CONTROLLED COPY' stamp, it is considered an uncontrolled working copy; the current version is maintained electronically."

Upon expiry of the relevant period, if there is no legal ground requiring further retention, personal data is deleted, destroyed, or anonymized. Necessary administrative and technical measures are taken to prevent the retention of data beyond the required period.

3.2. Conditions for Processing Personal Data

Article 5 of the Law No. 6698 on the Protection of Personal Data (KVKK) regulates the conditions for processing personal data. The Company carries out its personal data processing activities in compliance with the conditions set forth under the KVKK.

In addition to the explicit consent of the data subject, personal data processing activities may be based on one or more of the conditions listed below. Where the processed data qualifies as special categories of personal data, the conditions set forth under Section **3.3 of this Policy ("Processing of Special Categories of Personal Data")** shall apply.

3.2.1. Explicit Consent of the Data Subject

One of the legal bases for processing personal data is the explicit consent of the data subject. Such consent must be given in relation to a specific matter, based on adequate information, and expressed freely.

The Company shall carry out personal data processing activities in accordance with the explicit consent of the data subject, provided that such consent is obtained in a clear and unambiguous manner, following proper disclosure regarding the purposes of processing, as required under the KVKK, and limited to the scope of such consent.

In the presence of the following conditions, personal data may be processed without the explicit consent of the data subject:

i. Explicitly Provided for by Law

Pursuant to the KVKK, even in the absence of explicit consent, personal data may be processed where such processing is explicitly required by law, provided that other applicable conditions are also satisfied. In this context, personal data shall be processed by the Company within the limits set forth under the relevant legislation.

ii. Inability to Obtain Consent Due to De Facto Impossibility

Where the data subject is unable to provide consent due to a de facto impossibility, or where such consent is not legally valid, personal data may be processed where it is necessary to protect the life or physical integrity of the data subject or another person. The Company shall process personal data in accordance with such provisions where applicable.

iii. Directly Related to the Establishment or Performance of a Contract

Personal data belonging to the parties to a contract may be processed by the Company, provided that such processing is directly related to the establishment or performance of the contract.

iv. Fulfilment of the Company's Legal Obligations

Personal data may be processed by the Company, in its capacity as Data Controller, to the extent necessary for the fulfilment of its legal obligations arising from applicable legislation.

v. Data Made Public by the Data Subject

Where the data subject has made their personal data public, such data may be processed by the Company in a manner proportionate to the purpose of such disclosure.

vi. Necessity for the Establishment, Exercise, or Protection of a Right

Personal data may be processed to the extent necessary for the establishment, exercise, or protection of a legal right.

vii. Necessity for the Legitimate Interests of the Company,

Personal data may be processed for the legitimate interests of the Company, provided that such processing does not harm the fundamental rights and freedoms of the data subject.

However, the concept of "legitimate interest" shall in no case be interpreted or applied in a manner that is contrary to the principles set forth under the KVKK, the purpose of processing, or that infringes upon the essence of rights protected under the Constitution.

"If a printed copy of this document does not bear the 'CONTROLLED COPY' stamp, it is considered an uncontrolled working copy; the current version is maintained electronically."

3.3. Processing of Special Categories of Personal Data

IBS adopts additional safeguards determined by the Personal Data Protection Board when processing special categories of personal data. In the context of health insurance contracts, the health data of insured individuals is processed solely for the purposes of the contract and limited to such purposes.

Pursuant to Article 6 of the Law, data relating to an individual's race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dress, membership in associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data, are classified as special categories of personal data.

All business processes and documentation within the Company have been reviewed, and such data has been identified and classified accordingly.

Special categories of personal data are processed by the Company in accordance with the principles set forth in this Policy, by taking all necessary administrative and technical measures, including those prescribed by the Board, and under the following conditions:

(i) Explicit Consent of the Data Subject

As a general rule under the KVKK, special categories of personal data cannot be processed without the explicit consent of the data subject. Accordingly, the Company prioritizes obtaining the explicit consent of the data subject for the processing of such data. Processing activities are carried out within the scope of the consent provided.

(ii) Explicitly Provided for by Law

Where it is explicitly stipulated by law that special categories of personal data may be processed, such data—excluding data relating to health and sexual life—may be processed without the explicit consent of the data subject, in accordance with the KVKK.

In such cases, processing activities are strictly limited to the requirements of the relevant legislation. The submission of special categories of personal data within legal proceedings (such as lawsuits or enforcement proceedings), provided that such data is relevant and limited to the subject matter of the proceedings, as well as the collection of such data by courts, parties, or third parties and its retention for the duration required by such legal processes, shall be deemed processing based on legal grounds.

"If a printed copy of this document does not bear the 'CONTROLLED COPY' stamp, it is considered an uncontrolled working copy; the current version is maintained electronically."

(iii) Processing by Persons under Confidentiality Obligations for Public Health Purposes

Pursuant to the KVKK, the processing of personal data relating to health and sexual life is subject to explicit consent. However, in the absence of such consent, such data may only be processed by persons under a confidentiality obligation or authorized institutions and organizations, for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, and the planning, management, and financing of healthcare services.

Accordingly, the Company may process such data to the extent required by applicable legislation in situations where it is under a confidentiality obligation.

(iv) Necessity for the Fulfilment of Legal Obligations in Employment and Social Security Law

Processing may be carried out where it is necessary for the fulfilment of legal obligations relating to employment, occupational health and safety, social security, social services, and social assistance.

(v) Processing by Non-Profit Organizations

Processing may be carried out by foundations, associations, and other non-profit organizations established for political, philosophical, religious, or trade union purposes, provided that:

- it complies with applicable legislation and their purposes,
- is limited to their fields of activity, and
- is not disclosed to third parties,

and is limited to their current or former members or individuals who are in regular contact with such organizations.

3.3.1. Technical and Administrative Measures for the Secure Storage and Protection of Special Categories of Personal Data

Under the KVKK, it is mandatory to implement the measures determined by the Personal Data Protection Board for the processing of special categories of personal data.

IBS adopts all necessary technical and administrative measures to ensure that special categories of personal data are processed and destroyed in compliance with the law and the principles of good faith.

The Company processes such data in accordance with the measures prescribed by the Board.

"If a printed copy of this document does not bear the 'CONTROLLED COPY' stamp, it is considered an uncontrolled working copy; the current version is maintained electronically."

3.4. Informing the Data Subject

In accordance with Article 10 of the Law and secondary legislation, IBS informs data subjects accordingly. Within this scope, IBS provides information to the relevant persons regarding the identity of the data controller, the purposes for which personal data are processed, to whom and for what purposes the data may be transferred, the methods and legal grounds for data collection, and the rights of data subjects in relation to the processing of their personal data.

3.5. Transfer of Personal Data

The collection and processing of personal data shall be carried out in line with the purposes specified in the relevant information notices, and transfers shall be conducted accordingly.

Our Company may transfer personal data and special categories of personal data of the data subject to third parties (including third-party companies, public and private authorities, and natural persons), by taking the necessary security measures in line with lawful processing purposes. In this regard, our Company acts in compliance with the provisions set out in Article 8 of the Law. Detailed information on this matter can be found in **Annex 2 – Third Parties to Whom Personal Data Are Transferred and the Purposes of Transfer** of this Policy.

3.5.1. Transfer of Personal Data Within the Country

Even in the absence of the explicit consent of the data subject, personal data may be transferred to third parties by our Company, provided that one or more of the following conditions are met, with due care and by implementing all necessary security measures, including those prescribed by the Board:

- Where the transfer of personal data is explicitly stipulated by law,
- Where the transfer is directly related to and necessary for the establishment or performance of a contract,
- Where the transfer is mandatory for the Company to fulfill its legal obligations,
- Where the personal data have been made public by the data subject, limited to the purpose of such disclosure,
- Where the transfer is necessary for the establishment, exercise, or protection of the rights of the Company, the data subject, or third parties,

- Where the transfer is necessary for the legitimate interests of the Company, provided that it does not harm the fundamental rights and freedoms of the data subject,

- Where the transfer is necessary to protect the life or physical integrity of a person who is unable to give consent due to actual impossibility or whose consent is not legally valid.

3.5.2. Transfer of Personal Data Abroad

In addition to the above, personal data may be transferred to foreign countries that have been declared by the Board as having adequate protection **("Countries with Adequate Protection")**, in accordance with Article 9 of the Law, provided that any of the above conditions are met.

In the absence of adequate protection, transfers may be carried out based on appropriate safeguards as stipulated under Article 9 of the Law.

3.5.3. Transfer of Special Categories of Personal Data

Special categories of personal data may be transferred by our Company, in compliance with the principles set out in this Policy and by taking all necessary administrative and technical measures, including those determined by the Board, provided that the following conditions are met:

(i) Special categories of personal data other than those relating to health and sexual life may be processed without the explicit consent of the data subject where explicitly provided for by law. Otherwise, explicit consent shall be obtained.

(ii) Special categories of personal data relating to health and sexual life may be processed, without explicit consent, by persons under a duty of confidentiality or authorized institutions and organizations, for the purposes of protection of public health, preventive medicine, medical diagnosis, treatment and care services, and the planning and management of healthcare services and their financing. Otherwise, explicit consent shall be obtained.

In addition to the above, personal data may be transferred to Countries with Adequate Protection where any of the above conditions are met. In the absence of adequate protection, transfers may be carried out based on appropriate safeguards as regulated under Article 9 of the Law.

"If a printed copy of this document does not bear the 'CONTROLLED COPY' stamp, it is considered an uncontrolled working copy; the current version is maintained electronically."

4. CATEGORIZATION OF PERSONAL DATA PROCESSED BY OUR COMPANY AND PURPOSES OF PROCESSING

Within our Company, personal data are processed in accordance with the Law and secondary legislation, and by informing the relevant data subjects pursuant to Article 10 of the Law.

In line with our Company's personal data processing purposes, personal data are processed in a limited and proportionate manner, based on at least one of the personal data processing conditions set out in Articles 5 and 6 of the Law, and in compliance with the general principles stipulated under the Law, in particular the principles set out in Article 4 regarding the processing of personal data.

Within the scope of the purposes and conditions specified in this Policy, detailed information on the categories of personal data processed and such categories can be found in **Annex 3 – Retention and Destruction Periods of Personal Data Categories** of this Policy.

5. RETENTION AND DESTRUCTION OF PERSONAL DATA

Our Company retains personal data for the period required for the purpose for which they are processed and in accordance with the minimum retention periods stipulated under the applicable legislation governing the relevant activity.

In this context, our Company first determines whether a retention period is prescribed under the applicable legislation; if such a period exists, it complies with that period. If no legal retention period is specified, personal data are retained for the period necessary for the purpose of processing.

At the end of the applicable retention periods, personal data are destroyed in accordance with periodic destruction schedules or upon the request of the data subject, using the designated destruction methods (deletion and/or destruction and/or anonymization).

5.1. General Principles for Retention and Destruction of Personal Data

The Company is a Data Controller subject to registration in the Registry and undertakes to store personal data in accordance with the Personal Data Inventory and, where necessary, to delete, destroy, or anonymize such data in compliance with this Policy.

The following principles shall apply to the retention and destruction of personal data:

1. The Company shall comply with the general principles set out in Article 4 of the Law.

2. The Company acknowledges that the mere preparation of this Policy does not in itself mean that personal data are deleted, destroyed, or anonymized in compliance with the legislation.

3. The Company shall act in accordance with the security measures set out in Article 12 of the Law, the provisions of the applicable legislation, the decisions of the Board, and this Policy when storing, deleting, destroying, or anonymizing personal data.

4. The Company shall ensure compliance with this Policy and with the tools, programs, and processes to be implemented under this Policy when deleting, destroying, or anonymizing personal data processed wholly or partially by automated means or by non-automated means provided that they form part of a data recording system.

5. The Company shall record all transactions related to the deletion, destruction, and anonymization of personal data and shall retain such records for at least 3 (three) years, except where other legal obligations require otherwise.

The Company hereby accepts, declares, and undertakes the above.

5.2. Data Minimization Principle

Under the principle of data minimization, only data that are necessary are processed within the system. Accordingly, the data to be collected are determined based on the purpose, and unnecessary data are not collected.

Any additional data received by our Company are processed in the same manner; excess information is not recorded in the system and is either deleted or anonymized.

5.3. Legal, Technical, and Other Grounds Requiring Destruction of Personal Data

Personal data of data subjects may be deleted, destroyed, or anonymized by the Company in accordance with the general principles set out in Article 4 of the Law, in the following cases:

a) Upon the request of the data subject,

b) Upon the expiration of legal obligations.

5.4. Periodic Destruction

In addition to the retention and destruction periods specified in **Annex 3 – Retention and Destruction Periods of Personal Data Categories**, the periodic destruction period determined by the Company is 6 (six) months.

5.5. Deletion and Destruction Periods Upon Request of the Data Subject

If the data subject requests the deletion or destruction of their personal data by applying to the Company pursuant to Article 13 of the Law:

1. If all conditions for processing personal data have ceased to exist, the Company shall delete, destroy, or anonymize the personal data subject to the request. The Company shall finalize the request within 30 (thirty) days at the latest and inform the data subject accordingly.

2. If all conditions for processing personal data have ceased and the personal data have been transferred to third parties, the Company shall notify the relevant third party within 10 (ten) days and ensure that the necessary actions are taken by such third party.

3. If the conditions for processing personal data have not ceased, the request may be rejected by the Company with justification in accordance with Article 13/3 of the Law, and the rejection shall be communicated to the data subject in writing or electronically within 30 (thirty) days at the latest.

6. RIGHTS OF DATA SUBJECTS AND THE EXERCISE OF THESE RIGHTS

6.1. Rights of the Data Subject

IBS acknowledges that, under the Law, data subjects have the right to give consent prior to the processing of their personal data and, following such processing, to determine the fate of their personal data.

Pursuant to Article 11 of the Law, you have the following rights. To facilitate the exercise of these rights, an application form has been prepared by IBS Insurance and Reinsurance Brokerage Inc. and made available on our website.

Data subjects whose personal data are processed may submit their requests to IBS Insurance and Reinsurance Brokerage Inc., via the contact channels announced on our website, and request the following in relation to their personal data:

a) To learn whether their personal data are being processed,

b) To request information if their personal data have been processed,

c) To learn the purpose of processing of personal data and whether they are used in accordance with such purpose,

d) To know the third parties to whom personal data are transferred domestically or abroad,

e) To request the rectification of incomplete or inaccurate personal data,

f) To request the deletion or destruction of personal data in the event that the reasons requiring their processing no longer exist, even though they have been processed in accordance with the Law and other relevant legal provisions,

g) To request that the transactions carried out pursuant to subparagraphs (e) and (f) be notified to third parties to whom personal data have been transferred,

h) To object to the occurrence of a result against the person by analyzing the processed data exclusively through automated systems,

i) To request compensation for damages in case of loss due to unlawful processing of personal data.

6.2. Exercise of the Rights of the Data Subject

Data subjects may submit their requests regarding the rights listed under Section 6.1 (“Rights of the Data Subject”) to our Company through the methods determined by the Board.

For this purpose, they may use the **“IBS Data Subject Application Form”** available at: “https://www.ibsbroker.com.tr/en/legalinformation/Personal Data Protection Law - Application Form.pdf”

6.3. Response of Our Company to Applications

Our Company takes the necessary administrative and technical measures to ensure that applications submitted by data subjects are concluded in accordance with the Law and secondary legislation.

If the data subject duly submits a request regarding the rights specified in Section 6.1 (“Rights of the Data Subject”), our Company shall conclude the request free of charge as soon as possible and at the latest within 30 (thirty) days, depending on the nature of the request.

However, if the process requires additional costs, a fee may be charged in accordance with the tariff determined by the Board.

7. MATTERS RELATING TO THE PROTECTION OF PERSONAL DATA

7.1. Ensuring the Security of Personal Data

In accordance with Article 12 of the Law, our Company takes the necessary measures, appropriate to the nature of the data to be protected, to prevent unlawful disclosure, access, transfer, or any other security breaches that may occur in relation to personal data.

In this context, our Company implements the necessary technical and administrative measures to ensure an adequate level of security, in line with the guidelines issued by the Personal Data Protection Board (“Board”), and conducts or commissions the required audits.

7.2. Protection of Special Categories of Personal Data

Certain personal data are attributed special importance under the Law due to the risk of causing harm or discrimination if processed unlawfully. These include data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

IBS exercises utmost care in the protection of special categories of personal data defined under the Law and processed in compliance therewith.

In this regard, the technical and administrative measures implemented by IBS for the protection of personal data are applied with particular diligence in respect of special categories of personal data, and necessary audits are carried out within IBS.

Further details regarding the processing of special categories of personal data are provided in Section 3.3 (“Processing of Special Categories of Personal Data”) of this Policy.

7.3. Raising Awareness and Auditing of Business Units Regarding the Protection and Processing of Personal Data

IBS ensures that the necessary training is provided to its business units in order to raise awareness regarding the prevention of unlawful processing and access to personal data and to ensure the proper safeguarding of personal data.

Necessary systems are established to enhance employees’ awareness of personal data protection, and external consultants are engaged where required.

In this context, our Company evaluates participation in relevant training sessions, seminars, and information meetings, and updates and renews such training in line with changes in the applicable legislation.

In addition, IBS carries out the necessary internal and external audits concerning the protection of personal data.

7.4. Notification of Data Breaches

In the event that IBS is notified of any breach relating to personal data, it shall take immediate action to remedy such breach.

IBS shall minimize any damage suffered by the data subject and take steps to compensate for such damage.

Where personal data are obtained by unauthorized third parties, IBS shall promptly notify the Personal Data Protection Board.

“If a printed copy of this document does not bear the ‘CONTROLLED COPY’ stamp, it is considered an uncontrolled working copy; the current version is maintained electronically.”

8. PERSONAL DATA PROTECTION OFFICER

The contact details of the Company's Personal Data Protection Officer are as follows:

Name: İpek Gürtunca Arkun

Business Address: Maslak Mah. Eski Büyükdere Cad. Maslak Link Plaza No: 3-5, Maslak

Telephone: +90 212 272 45 72 / +90 533 955 38 68

Email: ipek.arkun@ibsbroker.com

9. ANNEXES

9.1. Annex 1 – Data Subjects

9.2. Annex 2 – Purposes of Personal Data Processing

9.3. Annex 3 – Retention and Destruction Periods of Personal Data Categories (Tables)

9.4. Annex 4 – Third Parties to Whom Personal Data Are Transferred and the Purposes of Transfer

ANNEX1 – Data Subjects

DATA SUBJECTS	DESCRIPTION
Employee	Company employees and former employees whose personal data are processed within the scope of activities carried out by the Company, such as employee engagement, human resources, audit, IT security and infrastructure, legal compliance, etc.
Job Applicant	Natural persons who have applied for a job at IBS through any means or have made their CVs and related information available for IBS's review.
Intern	Natural persons who maintain an ongoing relationship with an educational institution (such as a high school, university, or similar), and who carry out activities at IBS's workplace for a certain period for training purposes, not under an employment contract but within the scope of an internship agreement or protocol, and whose personal data are processed during this period.
Company Shareholder / Partner	Natural person shareholders of IBS.
Company Representative	Members of the board of directors and other authorized natural persons of IBS.
Customer (Person Receiving Products or Services)	Natural persons who purchase at least one of the products or services offered by IBS, establish a contractual relationship within this scope, or receive products or services for consideration, and whose personal data are processed during sales, after-sales support, and similar processes.
Prospective Customer (Potential Product or Service Recipient)	Natural persons who express interest in IBS's products or services, request information, receive offers, or share their personal data for communication within the scope of marketing activities, but have not yet entered into a purchase or contractual relationship.
Visitor	Natural persons who have entered IBS's physical premises for various purposes or who visit our websites.
Supplier Employee	Natural persons who are employees, representatives, or shareholders of parties providing services to IBS on a contractual basis, acting in accordance with IBS's instructions while carrying out IBS's commercial activities.
Supplier Representative	Natural persons working in institutions with which IBS has any kind of business relationship (such as business partners, suppliers, etc.), including their shareholders and authorized representatives.
Other	Other natural persons not covered under this Policy but whose personal data are processed within the scope of activities carried out by IBS (e.g., third parties, family members, relatives, etc.).

"If a printed copy of this document does not bear the 'CONTROLLED COPY' stamp, it is considered an uncontrolled working copy; the current version is maintained electronically."

EK 2 – Kişisel Veri İşleme Amaçları

MAIN PURPOSES	SUB-PURPOSES
Execution of Information Technology Processes	Execution of Information Security Processes
	Management of Access Authorizations
	Ensuring Business Continuity
	Ensuring the Security of Data Controller Operations
Execution of Human Resources Processes	Conducting Recruitment and Placement Processes for Job Applicants / Interns / Students
	Managing Job Application Processes
	Fulfillment of Employment Contract and Legal Obligations for Employees
	Management of Employee Benefits and Entitlements
	Employee Satisfaction and Engagement Processes
	Execution of Training Activities
	Assignment Processes
	Planning of Human Resources Processes
	Performance Evaluation Processes
	Tracking of Requests / Complaints
	Execution of Compensation (Remuneration) Policies
	Talent and Career Development Activities
Execution of Audit Activities	Execution of Audit / Ethics Activities
	Execution of Internal Audit / Investigation / Intelligence Activities
Execution of Business Operations	Ensuring Compliance with Legislation
	Execution of Finance and Accounting Processes
	Execution of Storage and Archiving Activities
	Management of Customer / Product / Service Loyalty
	Follow-up and Execution of Legal Affairs
	Receiving and Evaluating Suggestions for Improvement of Business Processes
	Execution of Procurement Processes for Goods / Services
	Execution of After-Sales Support Services
	Execution of Sales Processes for Goods / Services
	Execution of Production and Operational Processes
	Execution of Customer Relationship Management Processes
	Execution of Customer Satisfaction Activities
	Conducting Marketing Analysis Studies
	Execution of Contract Management Processes
	Tracking of Requests / Complaints
	Ensuring the Security of Movable Assets and Resources,
	Execution of Marketing Processes for Products / Services
	Providing Information to Authorized Persons, Institutions, and Authorities
Execution of Communication Activities	Organization and Event Management
	Other (Execution of Corporate Reputation Management Activities)
Execution of Management Activities	Execution of Strategic Planning Activities
	Execution of Risk Management Processes
	Execution of Investment Processes
Execution of Occupational Health and Safety Activities	Execution of Emergency Management Processes
	Ensuring Physical Premises Security

"If a printed copy of this document does not bear the 'CONTROLLED COPY' stamp, it is considered an uncontrolled working copy; the current version is maintained electronically."

Annex 3 – Retention and Destruction Periods of Personal Data Categories

The retention and destruction periods of the data processed by the Company have been determined based on the categories of personal data in the Personal Data Processing Inventory and are set out in the table below

TABLE A – PERSONAL DATA OF EMPLOYEES AND FORMER EMPLOYEES

PERSONAL DATA CATEGORY	DESCRIPTION	DATA PROCESSED BY IBS	RETENTION PERIOD	DESTRUCTION PERIOD
Identity	Includes data such as name-surname, parents' names, mother's maiden name, date/place of birth, marital status, ID details, etc.	Name, parents' names, date/place of birth, nationality, gender, marital status, ID/passport, tax number, population registry, marriage certificate, driver's license, etc.	10 years following termination of employment	Within 6 months after retention period
Contact	Includes address, email, phone, etc.	Address, residence address, email, phone number, etc.	10 years following termination of employment	Within 6 months
Location	Location data	Location data of employees using company vehicles	2 years	Within 6 months
Personnel (HR Data)	Payroll, recruitment, performance, disciplinary data, etc.	Payroll, employment records, CVs, applications, leave records, performance reports, disciplinary records, etc.	10 years following termination of employment	Within 6 months
Legal Transactions	Legal correspondence, case files, etc.	Contracts, legal correspondence, litigation records	10 years following termination of employment	Within 6 months
Physical Security	Entry/exit logs, CCTV	Access card records, CCTV recordings	10 years following termination of employment	Within 6 months
Transaction Security	IP, login records, passwords	IP data, login records, password info	10 years following termination of employment	Within 6 months
Risk Management	Risk-related data	Commercial, technical, administrative risk data	10 years following termination of employment	Within 6 months
Financial Data	Financial records, income, credit info	Bank account info (IBAN, branch, etc.), salary, debts/receivables, insurance/policy data, credit card info	10 years following termination of employment	Within 6 months
Professional Experience	Education, certificates, experience	CV data, diplomas, certificates, languages, past experience	10 years following termination of employment	Within 6 months
Audio / Visual Records	Photos, video recordings	ID photos, event photos/videos shared internally or on social media	10 years following termination of employment	Within 6 months
Special Categories of Personal Data	Health, criminal record, association membership	Health reports, blood group, criminal record, association membership data	10 years following termination of employment	Within 6 months
Other	Family, complaints, references	Family/emergency contacts, complaint records, reference info	10 years following termination of employment	Within 6 months

TABLE B – PERSONAL DARTA OF CUSTOMERS AN PROSPECTIVE CUSTOMERS

PERSONAL DATA CATEGORY	DESCRIPTION	DATA PROCESSED BY IBS	DESTRUCTION PERIOD	DESTRUCTION PERIOD
Identity	Includes data such as name-surname, parents' names, mother's maiden name, date/place of birth, marital status, ID details, etc.	Name, parents' names, date/place of birth, nationality, gender, marital status, marriage date, ID/passport details, tax number, population registry records, marriage certificate, driver's license, professional ID, etc.	10 years following termination of the business relationship	Within 6 months following the expiry of the retention period
Contact	Includes address, email, phone, etc.	Address, residence address, email address, contact address, phone number, etc.	10 years following termination of the business relationship	Within 6 months following the expiry of the retention period
Legal Transactions	Includes data related to correspondence with judicial authorities and litigation files	Contracts, legal correspondence, litigation records, etc.	10 years following termination of the business relationship	Within 6 months following the expiry of the retention period
Customer Transaction	Includes call center records, invoices, promissory notes, checks, receipts, order and request data	Insurance quotations, coverage details, policy information, etc.	10 years following termination of the business relationship	Within 6 months following the expiry of the retention period
Physical Premises Security	Includes entry/exit records and CCTV data	Access card system records and CCTV recordings within company premises	10 years following termination of the business relationship	Within 6 months following the expiry of the retention period
Transaction Security	Includes IP address, website access logs, passwords, etc.	IP address data, website login/logout records, password information	10 years following termination of the business relationship	Within 6 months following the expiry of the retention period
Risk Management	Includes data processed for managing commercial, technical, and administrative risks	Risk-related data for commercial, technical, and administrative purposes	10 years following termination of the business relationship	Within 6 months following the expiry of the retention period
Financial Data	Includes financial, credit, and asset-related data	Bank account details (IBAN, branch, account no.), insurance data, credit card data, income (salary, receivables/payables, tax number), financial performance data, assets, customer debt/limit data, policy quotations, customer collection data	10 years following termination of the business relationship	Within 6 months following the expiry of the retention period
Audio / Visual Records	Includes audio and visual recordings	Photos and video recordings taken during company events and shared on internal systems or social media	10 years following termination of the business relationship	Within 6 months following the expiry of the retention period
Special Categories of Personal Data	Includes health-related data such as disability status, blood group, medical data, etc.	Health reports, blood group information, medical data, prosthesis/device information, etc.	10 years following termination of the business relationship	Within 6 months following the expiry of the retention period
Other	**Vehicle Information** – includes vehicle data obtained for insurance purposes (e.g., license plate, registration details)	Vehicle-related insurance data	10 years following termination of the business relationship	Within 6 months following the expiry of the retention period
	Family and Relatives Information – includes emergency contact and health insurance-related data	Family member and relative information	10 years following termination of the business relationship	Within 6 months following the expiry of the retention period
	Request / Complaint Information – includes customer requests and complaints	Request and complaint records	10 years following termination of the business relationship	Within 6 months following the expiry of the retention period

Annex 4 – Third Parties to Whom Personal Data Are Transferred and the Purposes of Transfer

In accordance with Articles 8 and 9 of the Personal Data Protection Law, IBS may transfer the personal data of data subjects governed by this Policy to the following categories of recipients:

(i) IBS business partners,
(ii) IBS suppliers,
(iii) Legally authorized public institutions and organizations,
(iv) Legally authorized private legal entities.

The scope of such recipients and the purposes of data transfer are set out below:

RECIPIENTS OF PERSONAL DATA TRANSFER	DESCRIPTION	PURPOSE OF TRANSFER
Business Partners	Natural or legal persons with whom IBS cooperates to provide products or services, carry out joint projects, or conduct sales, marketing, operational, or support processes (e.g., insurance companies, reinsurance companies, domestic/international reinsurance brokers, loss adjusters, actuaries, etc.).	Limited to the purposes necessary for carrying out business activities, including: obtaining insurance quotations, issuing policies, managing claims and indemnity processes, renewal processes, reinsurance placements, risk sharing, securing coverage for large risks, ensuring reinsurance capacity, joint provision of products/services, execution of joint projects, management of sales and marketing processes, responding to customer requests, and providing operational and technical support.
Suppliers	Natural or legal persons providing goods or services to IBS in areas such as IT, infrastructure, human resources, consultancy, logistics, accounting, and similar fields.	Limited to ensuring the provision of outsourced services required for IBS's operations, including: execution of service and infrastructure processes, operation of IT systems, provision of support, maintenance and consultancy services, continuation of operational activities, fulfillment of contractual obligations, and operation of system infrastructure.
Authorized Public Institutions and Organizations	Public legal entities such as courts, public prosecutors, regulatory and supervisory authorities, ministries, and similar bodies authorized by law to request personal data.	Limited to the purposes requested within their legal authority, including: fulfilling legal reporting and notification obligations, conducting audits, complying with legal obligations, and responding to requests and inspections of competent authorities.
Authorized Private Legal Entities	Private legal entities authorized by law to request personal data, including independent auditors, authorized institutions, insurance companies, banks, and similar organizations.	Limited to the purposes within their legal authority, including: fulfillment of legal obligations, establishment, exercise or protection of legal rights, execution of financial transactions, audit, reporting and control processes, and carrying out financial and insurance-related transactions.

"If a printed copy of this document does not bear the 'CONTROLLED COPY' stamp, it is considered an uncontrolled working copy; the current version is maintained electronically."