IBS Sigorta ve Reasürans Brokerliği A.Ş.
PRIVACY POLICY

Validity Date : (01.01.2018)
Date of Update : (01.11.2021)

PREFACE

Dear Customers,

As IBS Sigorta ve Reasürans Brokerliği A.Ş. we meticulously keep the information of our valued customers and any personal data that left us by contacting us in any way.. We have taken all necessary measures within the company to ensure the security of your information. You can transact with IBS Sigorta ve Reasürans Brokerliği A.Ş. with the feeling that your personal data will be safe. We comply witth your rights regarding your data which are secured by both Constitution of The Republic of Turkey and the Laws. We share our Data Policy that has been put into force in our company in below.

You can be sure that we will show all sensitivity to your suggestions for improvement to your applications and possible complaints. You can apply to IBS Sigorta ve Reasürans Brokerliği A.Ş. for all your doubts regarding your personal data. We will show the same sensitivity and care in the protection of your personal data as in all our services.

Best regards

Purpose of The PrivacyPolicy

As IBS Sigorta ve Reasürans Brokerliği A.Ş. , we keep the data received from our insurant or potential customers confidential and never shared with third parties except for insurance transactions in accordance with the sensitivity of the work we have been dealing with. Protection of personal data is the main policy of our company. Our company attached great imporance to the privacy of personal data and adopted this as a working principle before there was any legal regulation.

Scope and Revision of the Privacy Policy

This Policy that prepared by our company has been prepared in accordance with the Law on the Protection of Personal Data No. 6698 (‘‘LPPD’’). The Law entered into force with all its provisions as of its publication.

The Privacy Policy of IBS Sigorta ve Reasürans Brokerliği A.Ş. aims to protect the personal data of our individual customers, corporate customer employees and other insured employees, employee candidates and our employees and includes regulations regarding these.

Our company reserves the right to change our policy and Regulations. Changes made to the policy will be marked in the text with the date and version code.

General Principles on Storage and Destruction of Personal Data

The Company , a Data Controller under LPPD, is obliged to register with the Registry and accepts, declares and undertakes that it is obliged to act in accordance with this Policy in order to store the personal data it holds in accordance with the Inventory and, if necessary to delete, destruct or anonymize it.

The following principles will apply to the storage and destruction of personal data:

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

2. The fact that the company has prepared this Policy does not by itself mean the deletion, destruction or anonymization of personal data in accordance with the legislation,

3. The Company will act in accordance with the security measures in Article 12 of the Law, the provisions of the relevant Legislation, Board decisions and the Policy while storing, deleting, destroying or anonymizing.

4. The Company ensure to compliance with the right to the tools, programs, and processes to be applied in accordance with this Policy, and destruction or anonymization of the personal data that is fully or partially automated or processed by non-automatic means if it is a part of any recording system during the deletion,

5. The Company will record all transactions regarding the deletion, destruction and anonymization of personal data and will keep the said records for at least 3 (three) years, excluding other legal obligations,

accepts, declares and undertakes.

You have the rights listed below according to Article 11 of LPPD. You can also send an application form to IBS Sigorta ve Reasürans Brokerliği A.Ş. prepared by us and presented to you on our website in order you to exercise these rights.

Persons whose personal data are processed by us, can apply to IBS Sigorta ve Reasürans Brokerliği A.Ş. by application form on the website . regarding their own data;

a) to learn whether his personal data are processed or not,

b) to request information if his personal data are processed,

c) to learn the purpose of his data processing and whether this data is used for intended purposes,

ç) to know the third parties to whom his personal data is transferred at home or abroad,

d) to request the rectification of the incomplete or inaccurate data, if any,

e) to request the erasure or destruction of his personal data under the conditions laid down in Article 7,

f) to request notification of the operations carried out in compliance with subparagraphs (d) and (e) to third parties to whom his personal data has been transferred,

g) to object to the processing, exclusively by automatic means, of his personal data, which leads to an unfavourable consequence for the data subject,

ğ) to request compensation for the damage arising from the unlawful processing of his personal data

Principle of Data Minimization

According to this principle which is called theprinciple of data minimization , the data received by IBS Sigorta ve Reasürans Brokerliği A.Ş. are only processed into the system as neceassary. Therefore, what data we collect is determined by the purpose. Unnecessary data is not collected. Other datas transmitted to our company are transferred to company information systems in the same way. Redundant information is not recorded in the system, deleted or anonymized.

Legal, Technical and Other Reasons Requiring the Destrucition of Personal Data:

Personal data belonging to the data subjects concerned by the Company within the general principles set forth in Article 4 of the Law;
a) The request of the data subject,
b) Termination of legal obligations,

destroyed for that reasons.

Techincal and Administrative Measures Taken For Safe Storage of Personal Data and Preventing Unlawful Processing and Access

The technical and administrative measures taken by the Company in order to keep the personal data belonging to the data subjects in a safe manner and to prevent their unlawful processing and access are listed below:

1. Closed system network is used for personal data transfers via network.
2. Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
3. There are disciplinary regulations that include data security provisions for employees.
4. Training and awareness activities are carried out periodically for employees on data security.
5. An authorization matrix has been created for the employees.
6. Access logs are kept regularly.
7. Institutional policies on access, information security, use, storage and destruction have been prepared and started to be implemented.
8. The authorizations of employees who change the job or quit their job in this field are removed.
9. Up-to-date anti-virus systems are used.
10. Firewalls are used.
11. Extra security measures are taken for personal data transferred via paper and the relevant document is sent in confidential document format.
12. Personal data security policies and procedures have been determined.
13. Personal data security issues are reported quickly.
14. Personal data security is monitored.
15. The security of physical environments containing personal data against external risks (fire, flood, etc.) is ensured.
16. The security of environmens containing personal data is ensured.
17. Personal data is reduced as much as possible.
18. Personal data is backed up and the security the backed up personal data is also ensured.
19. User account management and authorization control system is implemented and these are followed up.
20. Log records are kept without user intervention.

21. Existing risk and threats have been identified.

22. Protocols and procedures for special category personal data security have been determined and implemented.

23. If special category personal data is to be sent via e-mail, it must be sent in encrypted form and using REM or corportate mail account.

24. Secure encryption / cryptographic keys are used for special cateogry personal data and are managed by different units.

25. Instrusion detection and prevention systems are used.

26. Penetration test is applied.

27. Cyber security measures have been taken and their implementation is constantly monitored.

28. Encryption is used.

Technical and Administrative Measures Taken for the Erasureof Personal Data

Technical measures taken by the Company for the lawful erasureof personal data of data subjects,

1. Using the most up-to-date technologically necessary systems for the destruction of personal data, taking privacy and information security measures,

2. Closing eliminating the access, retrieval, re-use authorization and methods of the related users within the scope of personal data and removing the authority to restore the deleted data,

3. Irreversible deletion of personal data on the central server with cloud systems by issuing a deletion command,

4. Choosing the appropriate one among the methods of destruction (physical, demagnetization, overwriting) or anonymization for the technical recording media other than those listed according to the nature of the personal data,

5. Application of deletion (blackening, etc.), destruciton (physical destruction) methods for the destruction of personal data in non-technical recording media,

has been determined.

Administrative measures taken by the Company for the lawful erasure of personal data of data subjects,

1. To carry out the necessary implementation work on the destruction of personal data regularly,

2. To have the necessary equipment for the physical destruction of non-technical data recording media within the workplace of the Company,

has been determined.

Periodic Disposal

Periodic disposal periods are 6 (six) months, except for the periods specified in the table (ANNEX-1) showing the storage and destruction periods attached to this Policy, according to the categories of personal data processed by the Company.

Periods of Deletion and Destruction of Personal Data upon Request by the Data Subject

When the data subject requests the deletion or destruction of his/her personal data by applying to the Company pursuant to Article 13 of the Law;

1. If all the conditions for processing personal data have terminated; the Company deletes, destroys or anonymizes the personal data subject to the request. The Company finalizes the request of the data subject within 30 (thirty) days at the latest and informs the data subject.
2. If all the conditions for processing personal data have been terminated and the personal data subject to the request has been transferred to the third parties, the Company notifies the third party within 10 (ten) days at the latest; it ensures that the necessary actions are taken by the third party.
3. If all the conditions for processing personal data have not been terminated, this request may be rejected by the Company by explaining the reason in accordance with the thrid paragraph of Article 13 of the Law, and the refusal is notified to the data subject in writing or electronically within 30 (thirty) days at the latest.

Data Processing Purposes and Transfer to Third Parties

Personal data collection and processing of IBS Sigorta ve Reasürans Brokerliği A.Ş. will be carried out in line with the purposes specified in the clarification texts and the transfers will be made in the manner specified here.

Processing of Special Category of Personal Data

IBS Sigorta ve Reasürans Brokerliği A.Ş. also takes adequate measures determined by the Board in the processing of special category of personal data. Healt data of the insured are processed in line with the purpose of the contract for the contracting of health insurance.

IBS Sigorta ve Reasürans Brokerliği A.Ş. can only process special category of personal data for the purpose for which they were collected with the direct consent of individuals or the approval of third parties (for example, their employers) in cooperation with IBS in order to provide better services.

Technical and Administrative Measures Taken to Safely Store the Personal Data od Special Nature and to Prevent Unlawful Processing and Access

IBS Sigorta ve Reasürans Brokerliği A.Ş. takes all necessary technical and administrative measures in order to ensure that personal data of special nature is processed and destroyed in accordance with the law and good faith.

Additional technical and administrative measures taken regarding special category of personal data are as follows:

- If special category of personal data is to be sent via e-mail, it must be sent in encrypted form and using REM or corporate mail account.
- Secure encryption / cryptographic keys are used for special category of personal data and are managed by different units.
- Protocols and procedures for special category of personal data security have been determined and implemented.
- Up-to-date encryption/cryptographic keys are used for special category of personal data and are managed by different units.
- Data transfer is carried out by establishing a VPN between servers or using the sTFP method in transfers between servers in different physical environments, data transfer is carried out by establishing a VPN between servers or using the sTFP method.
- Transaction record of all movements performed on the data are securely logged.
- Continuous monitoring of the security updates of the environments where the data is located, regularly performing/having the necessary security tests and recording the test results.

Rights of the Data Subject

IBS Sigorta ve Reasürans Brokerliği A.Ş. accepts that the data subject has the right to obtain consent before the data is processed, and that it has the right to determine the fate of the data after the data is processed within the scope of the Law.

Regarding personal data by applying to our data subject announced on our website by IBS Sigorta ve Reasürans Brokerliği A.Ş. ;

a) Learning whether your personal data is processed or not,

b) Requesting information about personal data if your data has been processed,

c) Learning the purpose of processing personal data and whether they are used in accordance with its purpose,

d) Learning the third parties to whom personal data is transferred at domestically or abroad,

e) Requesting correction of personal data in case of incomplete or incorrect processing,

f) Requesting the deletion or destruction of personal data within the framework of the conditions stipulated in the law,

g) Requesting notification of the transactions made pursuant to subparagraphs (d) and (e) to third parties to whom personal data has been transferred,

h) Objecting to the emergence of a result against the person himself by analyzing the processed data exclusively through automated systems,

i) Requesting the compensation of the damage in case of loss due to the unlawful processing of personal data,

has rights.

Audit

IBS Sigorta ve Reasürans Brokerliği A.Ş. carries out the necessary internal and external audits regarding the protection of personal data.

Notification of Breach

When IBS Sigorta ve Reasürans Brokerliği A.Ş. is notified of any breach of personal data, it takes immediate action to remedy the breach. It minimizes the harm of the data subject and compensates the damage of her/him. Notifies the Personal Data Protection Board immediately when personal data is obtained by unauhorized persons.

ANNEX-1 STORAGE AND DISPOSAL TIMES TABLES

The storage and destruction periods of the data processed by the Company have been determined based on the category of personal data in the Personal Data Porcessing Inventory and are given in the table below.

TABLE A – TABLE OF PERSONAL DATA OF EMPLOYESS AND FORMER EMPLOYESS

CATEGORY OF PERSONAL DATA	**PERSONAL DATA IN THE CATEGORY**	**STORAGE PERIOD**	**DISPOSAL TIME**
Identity	Name, surname, mother's maiden name, date of birth, date of marriage, place of birth, marital status, identity card, serial number, TR identity number, passport information etc., driver's licence	15 year from the end of the employment relationship	Within 6 Months following the end of storage period
Contact	Address no, e-mail address, contact address, residence, telephone number etc.	15 year from the end of the employment relationship	Within 6 Months following the end of storage period
Personnel	Payroll information, disciplinary investigation, employment entry-exit document records, property declaration information, CV information, name-surname of dependents and T.R. No, performance evaluation reports etc., salary information, position, date of departure, notice of period, reason for leaving the job, instant converstation details	15 year from the end of the employment relationship	Within 6 Months following the end of storage period
SSI	Registariton number	15 year from the end of the employment relationship	Within 6 Months following the end of storage period
Military Service	Military service information	15 year from the end of the employment relationship	Within 6 Months following the end of storage period
Legal Action	Employment contract, permission form, advance form, petition, complaint	15 year from the end of the employment relationship	Within 6 Months following the end of storage period
Experience of Profession	Previous professional experience, previous projects	15 year from the end of the employment relationship	Within 6 Months following the end of storage period
Education	Foreign languages spoken, schools attended and trainings received, diplomas, graduation date, occupational safety and fire certificates	15 year from the end of the employment relationship	Within 6 Months following the end of storage period
Visual Record	Photograph	15 year from the end of the employment relationship	Within 6 Months following the end of storage period

Finance	Bank account information, IBAN, bank branch name, branch code	15 year from the end of the employment relationship	Within 6 Months following the end of storage period
Performance	Name and surname, department, task, competency evaluation, evaluation of business processes, comments of the employee, comments of the manager	15 year from the end of the employment relationship	Within 6 Months following the end of storage period
Permission Forms	Name and surname, date of leave, reason for permission, place of leave, contact information	15 year from the end of the employment relationship	Within 6 Months following the end of storage period
Health Informations	Information on disability status, blood group information, blood count, lung examination and eye report, disability report	15 year from the end of the employment relationship	Within 6 Months following the end of storage period
Criminal Conviction and Security Measures	Information on criminal convictions, information on security measures etc.	10 year from the end of the employment relationship	Within 6 Months following the end of storage period
Others	Name and surname of the employee in the insurance sector, target information of the employee, evaluation reports	15 year from the end of the employment relationship	Within 6 Months following the end of storage period

TABLE B – TABLE OF PERSONAL DATA OF CUSTOMERS AND POTENTIAL CUSTOMERS

CATEGORY OF PERSONAL DATA	**PERSONAL DATA IN THE CATEGORY**	**STORAGE PERIOD**	**DISPOSAL TIME**
Identity	Name-surname, title, date of birth, mother's maiden name, T.R. Identitiy Number, marital status	10 years from the end of the commercial relationship	Within 6 Months following the end of storage period
Contact	Telephone number, e-mail address, address, risk address, residence information	10 years from the end of the commercial relationship	Within 6 Months following the end of storage period
Finance	Bank account number, insurance information, copy of policy, CCV, Salary, IBAN, Credit cart information	10 years from the end of the commercial relationship	15 years from the end of the commercial relationship
Education	Occupational information	10 years from the end of the commercial relationship	Within 6 Months following the end of storage period
Visual Record	Photograph	10 years from the end of the commercial relationship	Within 6 Months following the end of storage period

Health Information	Data of Health	10 years from the end of the commercial relationship	Within 6 Months following the end of storage period
Criminal Conviction and Security Measures	Information on criminal convictions, information on security measures etc.	10 years from the end of the commercial relationship	Within 6 Months following the end of storage period
Religion Information	Religion Information	10 years from the end of the commercial relationship	Within 6 Months following the end of storage period
Race Information	Race Information	10 years from the end of the commercial relationship	Within 6 Months following the end of storage period
Others	Vehicle license, title deed, risk address, fire and theft security information, damage data for the last 3 years, photos of private use areas (in addition to the appraisal report), driver's license, insurance information, vehicle information, housing details, auto accident history, business card, tax plate,	10 years from the end of the commercial relationship	Within 6 Months following the end of storage period

TABLE C – TABLE OF SUPPLIERS' PERSONAL DATA

CATEGORY OF PERSONAL DATA	PERSONAL DATA IN THE CATEGORY	STORAGE PERIOD	DISPOSAL TIME
Identity	Name, surname, title, T.R. ID Number, copy of ID	10 years from the end of the commercial relationship	Within 6 Months following the end of storage period
Contact	Phone number, e-mail address, contact address	10 years from the end of the commercial relationship	Within 6 Months following the end of storage period
Finance	Tax number information	10 years from the end of the commercial relationship	Within 6 Months following the end of storage period

ANNEX 2: TABLE OF OFFICIAL DEPARTMENS AND INFORMATIONS

The titles, departmens and job descriptions of the Company employees involved in the storage and destruction of personal data are given in the table below.

Only job descriptions on the protection of personal data of all employees listed below are included, and all of them have the duty to ensure compliance with the retention periods of personal data concerning the processes included in their job descriptions.

TITLE	**DEPARTMENT**	**JOB DESCRIPTION**
General Manager	Administration	It is responsible for the implementation of administrative decisions required for the company to act in accordance with the legislation.
Financial and Administrator Assistant General Manager	Administration	It is responsible for the company's employees to act in accordance with the LPPD and relevant legisations, to carry out training and awareness activities about the legislation, and to process personal data of employees in accordance with the legislation.
Deputy General Manager	Administration	It is responsible for conducting periodic and/or random internal supervisions regarding whether the company and its employees act in accordance with the LPPD or not.
Deputy General Manager	Administration	The employee of the company is responsible for the processing and destruction of health data which is within the scope of special category of personal data of the data subject.
Deputy General Manager	Administration	It is responsible for the desturction of the stored personal data determined by the company in non-technical data recording media (paper, department cabintes, archive) and reporting after destruction.