

### DEFINITIONS

In this Policy the following definitions shall apply:

1. "Applicable law" means the applicable legislation of the European Union and the Republic of Bulgaria relevant to the protection of personal data;
2. "General Data Protection Regulation" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
3. "Personal data" means any information relating to an identified or identifiable natural person who can be identified;
4. "Processing" means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, modification, use, disclosure by transmission or otherwise making available;
5. "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.
6. "Personal data register" means any structured set of personal data that is available under defined criteria;
7. "Data controller" means the natural or legal person, public authority or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
8. "Data processor" means the natural or legal person, public authority or other body which processes personal data on the data controller's behalf.
9. "Consent of the data subject" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
10. "Person Disclosing Personal Data" means the natural or legal person, public authority or other body which discloses personal data to the Recipient of Personal Data;
11. "Recipient of personal data" means the natural or legal person, public authority or other body which receives personal data from the Person disclosing Personal Data;
12. The terms "data subject", "personal data breach," "processing", "special categories of personal data" and "supervisory authority" shall have the meaning given to them under GDPR and the applicable local legislation.

### Section I

#### GENERAL PROVISIONS

**Art. 1.** This policy on personal data protection determines the rules for the protection of natural persons in relation to the processing of their personal data, as well as the rules for free movement of such data in accordance with the requirements of Regulation (EU) 2016/679 of the European Parliament

**Art. 2.** This policy determines the purposes and means of protection of personal data. The aim of the policy is achieved through:

1. Establishing clear rules and coordination in the activities of the employees of ZEAD Bulstrad Vienna Insurance Group in collecting, recording, organizing, structuring, storing, modifying, using, disclosing by transmission, releasing, restricting or deleting data in the registers kept by the company, in order to guarantee the integrity of the rights of data subjects during the processing of personal data of data subjects;
2. Establishing clear rules for the exercise of the rights of data subjects regarding their personal data;
3. Determination of a Data Protection Officer and designation of his or her responsibilities;
4. Regulation of the access of employees to data in the respective Register of processing activities;
5. Determination of Registers of processing activities;
6. Regulation of the principles to be observed in data management;
7. Determination of the necessary technical and organizational measures to protect personal data from unlawful processing (accidental or unlawful destruction, accidental loss, unauthorized access, alteration or dissemination, as well as from all other unlawful forms of processing of personal data);
8. Determining the levels of impact on personal data processed and the corresponding level of protection.

**Art. 3.** These rules regulate:

1. The principles in the activity of ZEAD Bulstrad Vienna Insurance Group as a data controller, in accordance with the requirements of Regulation (EU) 2016/679 of the European Parliament, the Personal Data Protection Act and applicable law.
2. The mechanisms governing the implementation of and compliance with the above principles
3. The rights of data subjects and the procedures for exercising the rights of data subjects;
4. The functions of ZEAD Bulstrad Vienna Insurance Group as a data controller;
5. The relations of ZEAD Bulstrad Vienna Insurance Group with companies which also act, by virtue of a contract, as data controllers or data processors;
6. Data protection impact assessment and determining the levels of impact on and protection of the processed personal data.

### Section II

#### PRINCIPLES RELATED TO THE PROCESSING AND PROTECTION OF PERSONAL DATA

**Art. 4. (1)** The main principles of the activity of personal data by ZEAD Bulstrad Vienna Insurance Group are:

1. Lawfulness, fairness and transparency of personal data processing. In order for processing to be lawful and fair, personal data should be processed on specific lawful grounds, in accordance with the requirements of Regulation (EU) 2016/679 of the European Parliament or a legal act of the Republic of Bulgaria governing the matter, as follows:
  - 1.1. Based on a legitimate interest of the company;
  - 1.2. For complying with a legal obligation imposed on the company in its capacity of data controller;

1.3. For the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

1.4. Based on an explicit consent of the data subject.

Applying the principle of transparency requires that any information and communication related to personal data processing shall be concise, easily accessible and easy to understand, and that clear and plain language be used;

2. Purpose limitation. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Data minimization. The personal data collected shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accuracy. The personal data collected and processed by the company shall be accurate and, where necessary, kept up to date, whereas the company shall undertake every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. Storage limitation. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods only for statistical purposes of the company, subject to implementation of the appropriate technical and organizational measures in order to safeguard the rights and freedoms of the data subject
6. Integrity and confidentiality. Personal data shall be processed in a manner that ensures appropriate level of security of the personal data. The company uses appropriate technical or organizational measures for this purpose.

**(2)** ZEAD Bulstrad Vienna Insurance Group collects, processes, and stores the personal data of data subjects:

1. Ensuring respect for the personhood and privacy of data subjects during the processing of their personal data;
2. According to lawful and fair processing of the data;
3. Ensuring that data is processed only by persons whose official duties require the processing of the specific data on a need-to-know basis. Data protection measures are a function of the type of data register and the sensitivity level of the data.

**(3)** In order to ensure storage limitation of the data, the company has established and applies its internal rules on document archival.

**Art. 5 (1).** ZEAD Bulstrad Vienna Insurance Group does not process personal data:

1. revealing racial or ethnic origin;
2. revealing political opinions, religious or philosophical beliefs; political party or trade-union membership or membership in associations with religious, philosophical, political or trade-union purposes;
3. related to genetic or biometric data processed solely to identify a human being;
4. concerning a person's sex life or sexual orientation or the human genome.

**(2)** The types of personal data specified in the paragraph above may be processed by the company only on legal grounds.

**Art. 6.** Health-related personal data are processed in accordance with the requirements of Regulation (EU) 2016/679 of the European Parliament and/or a legal act of the Republic of Bulgaria regulating such matter.

**Art. 7. (1).** ZEAD Bulstrad Vienna Insurance Group may process personal data alone or through third parties in their capacity of data processors

or joint controllers on the basis of a contract concluded with them. The respective contract shall specify clearly and accurately the personal data to be processed, the period and the purpose of processing.

**(2)** Processing of the personal data of data shall be performed in accordance with professional confidentiality. This is a mandatory requirement regarding the relations between employees, between employees and customers, as well as with respect to third party data processors and joint controllers.

**(3)** Whether ZEAD Bulstrad Vienna Insurance Group processes personal data alone or through third parties in their capacity of data processors or joint controllers, their processing is subject to the observance of the principles under Art. 4 of this policy at all times.

## Section III

### RIGHTS OF DATA SUBJECTS

**Art. 8. (1).** The rights of data subjects extend to the entire personal data of natural persons processed by ZEAD BULSTRAD VIENNA INSURANCE GROUP, as well as to all data subjects whose data are processed by the company

**(2)** The basic rights of data subjects, established by the legal framework and observed by the company, are the following:

1. Right of access;
2. Right to rectification;
3. Right to erasure (right to be forgotten);
4. Right to restriction of processing;
5. Right to object to the processing of personal data;
6. Right of the data subject not to be subject to a decision based solely on automated processing;
7. Right to data portability.

**Art. 9. (1).** The right to access data represents the right of the data subject to receive from ZEAD BULSTRAD VIENNA INSURANCE GROUP as data controller, a confirmation whether personal data relating to him or her is being processed and, if so, to obtain access to his or her personal data and the following information:

1. purposes of processing;
2. categories of personal data concerned;
3. categories of recipients to whom the personal data have been or will be disclosed;
4. envisaged period of storing the personal data, or, if not applicable, the criteria used for determining this period;
5. existence of the right to request from the company rectification or erasure of the personal data concerning the data subject or restriction of its processing, or the right to object to its processing;
6. right to lodge a complaint with a supervisory body;
7. where the personal data are not collected directly from the data subject, any available information as to their source;
8. existence of automated decision-making, including profiling, and information on the logic involved, as well as significance and envisaged consequences of such processing for the data subject;

**Art. 10.** Data subjects have the right to request from ZEAD BULSTRAD VIENNA INSURANCE GROUP that their personal data be rectified if the data are inaccurate or incomplete. Regarding any error existing in the data processed by the Company, it is obliged to honor this request and further inform the other recipients of such data to rectify the data too.

**Art. 11. (1).** Data subjects have the right to erasure (the right to be forgotten) of their data in case:

1. the data are no longer necessary for their initial purpose and there is

- no new lawful purpose;
- 2. in case the legal basis for the processing is the subject's consent and the data subject has withdrawn that consent, whereas there is no other legal basis for such processing;
- 3. the data subject objects to the processing and there is no other legal basis for such processing;
- 4. the personal data have been processed unlawfully;
- 5. the personal data is to be erased in order to meet a legal obligation arising from legislation applicable to the company;
- 6. the personal data have been collected in relation to the offer of information society services to data subject who is a child;

**(2)** The company shall not apply the right to erasure of personal data to the extent that the processing is necessary:

1. for compliance of the company with a legal obligation under legislation that requires processing of such data;
2. for the establishment, exercise or defense of legal claims.

**Art. 12. (1).** Data subjects have the right to request from the company to restrict the processing of their data in the following cases:

1. the accuracy of the personal data is contested by the data subject, whereas the restriction concerns a period that allows the company to verify the accuracy of the personal data;
2. the processing is not lawful, but the data subject does not wish his or her personal data to be erased, instead requesting restriction of the data's use.
3. When the company no longer needs the personal data for the purposes of processing, but the data subject has requested them for establishment, exercise or defense of legal claims;
4. The data subject has objected to the processing and is awaiting verification by the company whether the company's legitimate grounds override his or her own interests.

**(2)** When processing is restricted in accordance with par. 1, such data shall be processed (other than their storage) only with the consent of the data subject or when necessary for the establishment, exercise or defense of legal claims, or for the protection of the rights of other individuals, or for important reasons of public interest.

**(3)** When the data subject has exercised his or her rights to rectification, erasure or restriction of processing and the company has rectified its records accordingly, the company is obliged to communicate those actions to any recipient of such personal data, unless this is not possible or requires a disproportionate effort.

**Art.13. (1).** The data subject has the right to object at any time to the processing of personal data related to him or her, where such processing is based on the legitimate interest of the company. In such case, it is possible that ZEAD BULSTRAD VIENNA INSURANCE GROUP may not cease the processing in case of legal grounds which override the interests, rights and freedoms of the data subject, or in case the processing is necessary for the establishment, exercise or defense of legal claims.

**(2)** In case the data subject objects to the processing of his or her personal data for direct marketing purposes, the company shall cease the processing for that purpose.

**Art. 14.** The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. This rule shall not apply if the decision is necessary for the conclusion or performance of a contract between the company and the data subject.

**Art. 15. (1).** The data subject has the right to receive personal data related to him or her, which he or she has provided to the company, in a structured, commonly used and machine-readable format, as well as the

right to transfer such data to another controller.

**(2).** In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly by ZEAD BULSTRAD VIENNA INSURANCE GROUP to another controller, only where technically feasible.

**Art. 16.** For the exercise of the rights of data subjects with respect to their data, the company has established and applies Rules for the exercising the rights of data subjects.

## Section IV

### DATA PROTECTION IMPACT ASSESSMENT

**Art. 17. (1).** Whenever processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the company shall carry out an impact assessment of the intended operations.

**(2)** The impact assessment shall comprise, as a minimum, the following:

1. A systematic description of the envisaged processing operations and the purposes of processing;
2. An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
3. Assessment of the risks to the rights and freedoms of data subjects;
4. The measures envisaged to address the risks, including security measures and mechanisms to ensure the protection of personal data

**Art. 18.** The impact assessment procedure shall be conducted in accordance with the principles of purposefulness, thoroughness, comprehensiveness and timeliness:

1. The principle of "purposefulness" refers to the obligation of the Company to carry out the assessment procedure with respect of each maintained personal data register;
2. The principle of "thoroughness" refers to the obligation of the Company to review the nature of the processed personal data organized into registers;
3. The principle of "comprehensiveness" refers to the obligation of the Company to carry out the general assessment procedure in respect of all personal data registers it maintains;
4. The principle of "timeliness" requires the Company to carry out the assessment procedure without delay in case of any change in the nature of the personal data processed and the number of impacted individuals.

**Art. 19.** An impact assessment shall be carried out regularly every 2 years, and whenever there is a change in the nature of processed personal data.

## Section V

### REGISTERS OF THE PROCESSING OPERATIONS

**Art. 20. (1).** This section lists the indicative requirements in the processing of personal data, depending on the kind of register medium and level of sensitivity of the data.

**Art. 21. (1).** ZEAD BULSTRAD VIENNA INSURANCE GROUP, as data controller, shall keep the following indicative registers:

1. "Client files" register for insurance contracts concluded by ZEAD BULSTRAD VIENNA INSURANCE GROUP and insurance files / claims/. It is used to process personal data of the company's customers, parties to /or their representatives/ and beneficiaries of insurance contracts.
2. "Human Resources Management" register, established for administration of the activity of ZEAD BULSTRAD VIENNA INSURANCE GROUP in relation to staff management. It is used to process personal

data of company employees, as well as personal data of job applicants and interns;

3. Register of "Brokerage contracts" of ZEAD BULSTRAD VIENA INSURANCE GROUP or offers for conclusion of such contracts. It is used to process the personal data of counterparties or persons related to the company business;
4. Register of the data processing operations of ZEAD BULSTRAD VIENA INSURANCE GROUP for "Proceedings, files and complaints". It is used for processing the personal data of persons related to or affected by the company business, including during the conclusion, servicing, exercise of rights under and discharge of obligations under contracts and related claims; responses to complaints and inquiries from persons who are not customers of the company;;
5. Register of the "Administrative services"/access control/ designed for provision of security at ZEAD BULSTRAD VIENA INSURANCE GROUP and for worktime monitoring. It is used for processing the personal data of employees, customers and other persons who cross the streets adjacent to the company buildings.
6. Register of "Procurement contracts" for contracts of ZEAD BULSTRAD VIENA INSURANCE GROUP with external providers. It shall be used for the processing of personal data of counterparties and/or persons under contracts with external service providers, trusted medical professionals, external experts, etc. who provide assistance for the company business.

(2) In accordance with the procedure provided by the law and with the company operations, other registers may be established too, and those listed above may be named or organized differently.

(3) The personal data in the above registers shall be collected, processed and stored by the respective specialists involved in the process of administering and servicing the relevant activity of the company.

**Art. 22.** The minimum requirements for registers maintained on paper are:

1. Storage of the media in lockable rooms that are inaccessible to outsiders and, where necessary, in locking security cabinets;
2. Upon expiry of the reason or purpose of the processing, as well as of the storage period, the disposal of such documents shall be carried out in a way as to preclude any further readability of the data.
3. Persons with direct access to documents containing personal data shall immediately notify their line manager, who shall in turn notify the Data Protection Officer in the event of discovery of any unauthorized access to or use of information comprising personal data or of any unauthorized entry into premises where such information is stored.
4. The measures under the items above shall be observed also by the employees who, in the performance of their duties, have requested the provision of such information from the employees in whose custody the collected data are initially maintained.
5. The Data Protection Officer of ZEAD BULSTRAD VIENA INSURANCE GROUP shall maintain information on signals and incidents related to the previous paragraph, analyze the omissions and propose measures for their correction.
6. The archival of documents shall be subject to the internal rules on document archival at ZEAD BULSTRAD VIENA INSURANCE GROUP.
7. The access to and extraction of data from these registers shall be conducted, whenever possible, without removing the original media from the premises where they are stored.

**Art. 23.** The data maintained in the electronic systems of ZEAD BULSTRAD VIENA INSURANCE GROUP shall be stored either on a local computer or a network not connected to the public network. They shall be subject to the respective organizational and technical measures

for personal data protection.

**Art. 24.** The registers subject to the respective organizational and technical measures for personal data protection all comprise electronic data sets containing customer data and data on other persons related to the services of ZEAD BULSTRAD VIENA INSURANCE GROUP.

**Art. 25.** The protection of systems, use of passwords, access restrictions and rules for the work with the systems, the specification of technical resources applied in data processing, the procedure for storing and destroying media with data, as well as the procedure for backup and recovery of data in the event of loss, are in compliance with the approved internal rules and instructions of ZEAD BULSTRAD VIENA INSURANCE GROUP.

## Section VI

### DATA PROTECTION OFFICER

**Art. 26. (1).** On account of the nature, scope and objectives of data processing operations which require regular and systematic large-scale monitoring of data subjects, the need to process special data categories and for compliance with the legal requirements, ZEAD BULSTRAD VIENA INSURANCE GROUP has appointed a Data Protection Officer (DPO), whose objective is the control over the processing operations and assurance that the company meets its obligation to protect the personal data of data subjects.

(2) The DPO is appointed with a decision of the Management Board of the company.

(3) All structural units of ZEAD BULSTRAD VIENA INSURANCE GROUP are obliged to provide support to the DPO and observe his or her recommendations in relation to the processing and protection of personal data.

(4) Data subjects may contact the DPO with regard to all issues related to the processing of their personal data and the exercise of their rights under the law.

**Art. 27.** The DPO is subject to the following requirements:

1. The DPO shall be independent, shall not receive any instructions in relation to the performance of his or her tasks and shall not be dismissed or sanctioned by the company or by a processor for the performance of his or her tasks.
2. The DPO may fulfil other tasks and duties provided that they do not result in a conflict of interests.
3. The DPO is bound by secrecy or confidentiality in the performance of his or her tasks in accordance with the legal requirements.

**Art. 28. (1).** Duties of the Data Protection Officer:

1. To inform and give advice to the company, data processors and their employees of their obligations regarding personal data protection;
2. To monitor the compliance with the legislation related to personal data protection and the company Policy on personal data protection, including assignment of responsibilities, awareness-raising and provision of training to the staff involved in processing operations;
3. To provide advice upon request with regard to data protection impact assessments;
4. Whenever necessary, to give recommendations regarding the organization of register keeping and access rights of employees, in accordance with the adopted measures for ensuring adequate protection;
5. To assist the supervisory bodies, in particular the Commission for Personal Data Protection (CPDP) and liaise with CPDP regarding the measures and means adopted for protection of the registers and the requests submitted for provision of personal data;

6. To assist in the establishment of circumstances regarding breaches of the registers' protection.
- (2). The Director of IT Department and the Director of Legal Department shall support the DPO in the performance of his or her duties.
- (3). The company shall support the DPO with regard to the performance of the duties under par. 1 by providing the necessary resources, access to the personal data and the processing operations, as well as support for maintaining knowledge and expertise.

## Section VII

### PROCEDURE ON THE ACCESS TO PERSONAL DATA BY DATA SUBJECTS OR THIRD PARTIES. OBJECTIONS AND COMPLAINTS SUBMISSION. GENERAL PROVISIONS ON THE REVIEW OF REQUESTS AND COMPLAINTS RELATED TO PERSONAL DATA

**Art. 29. (1).** All signals from subjects with regard to personal data shall be entered in the document registry unit of ZEAD BULSTRAD VIENA INSURANCE GROUP and registered in register of complaints.

(2) Customers may submit a request for access to personal data through all channels for submission of requests, complaints or objections, in compliance with the Rules on exercising the rights of data subjects of ZEAD BULSTRAD VIENA INSURANCE GROUP.

(3) ZEAD BULSTRAD VIENA INSURANCE GROUP shall give its response within 1 month from receiving the request, compliant or objection.

(4) The unit and/or Department in charge of processing the specific database and servicing the specific operations referred to in the complaint shall prepare a response to the data subject and, if necessary, coordinate the response with the DPO. The decision regarding a request, complaint or objection shall be communicated to the head of the respective unit for the purpose of applying the measures prescribed by the IT Security Committee, if any.

(5) The exercise of the rights of data subjects under this Section shall be subject to the provisions of the Rules on exercising the rights of data subjects.

**Art. 30.** Any data subject may submit a request to the company for the exercise of his or her rights, in accordance with Section III of this Policy.

**Art. 31.** In case of requested access to classified information, such access shall be denied.

**Art. 32.** In case of a request from a third party for access to the personal data of customers of ZEAD BULSTRAD VIENA INSURANCE GROUP which does not represent secret or classified information, the requested data will be provided only where the following conditions are met at the same time.

1. The person requesting the data has a legal interest;
2. It cannot be concluded that the interests of the data subject override the interests of the person requesting the disclosure of data;
3. The data recipient falls in a category of persons regarding whom the data subject has been informed in advance of the possibility of disclosure of his or her personal data, or the data subject has received a notification of the disclosure of his or her personal data after the receipt of the third party request at the company;
4. The data subject has given his or her explicit written consent to the disclosure.

**Art. 33.** In case the requested data contain secret or classified information, the requirements prohibiting such disclosure shall be upheld.

**Art. 34. (1)** In case of a request is made by a public authority for provision of information which also contains personal data, the specific normative act regulating the procedure for provision of such information shall be applied.

(2) Where a letter with a request from a public authority contains personal data already individualizing certain subjects, the letter-response shall not include more data individualizing the customers, unless such data are required by the authority.

**Art. 35.** Data subjects may make an objection or submit a request to ZEAD BULSTRAD VIENA INSURANCE GROUP, as follows:

1. Objection to the processing of their personal data where there is a legal basis for doing so; if the objection has valid grounds, the personal data of the data subject concerned may no longer be processed;
2. Objection to the processing of their personal data for direct marketing purposes, notwithstanding the initially expressed written consent;
3. Request to be notified before their personal data are first disclosed to third parties, notwithstanding the subject's initial written consent, with provided opportunity to object to such disclosure or use. In the event that not making such disclosure or use would hinder the discharge of obligations under an insurance contract, the contract shall be terminated and the customer notified thereof.
4. In case the data subject has not made such request under the item above to be notified prior to any disclosure of personal data, he or she may still object to the disclosure and the respective insurance contract will be terminated.

## Section VIII

### TRANSFER, VERIFICATION AND JOINT PROCESSING OF PERSONAL DATA BETWEEN ZEAD BULSTRAD VIENA INSURANCE GROUP AND ANOTHER CONTROLLER

**Art. 36. (1).** The transfer of personal data by ZEAD BULSTRAD VIENA INSURANCE GROUP to other controllers, including in EU member states, pursuant to an agreement, shall be made in accordance with the conditions and options set out in these Rules and, in the absence of prior notification to the data subject about the possible categories of data recipients, he or she shall be notified about the disclosure immediately before or after it is made.

(2) The notification under par. 1 above shall contain the following information:

1. Categories of the personal data transferred;
2. Recipient of the data;
3. Purposes of the processing.

(3) When data is transferred to a recipient in a non-EU country, this shall be subject to the specific requirement of the Law governing such transfers.

**Art. 37.** During negotiation and conclusion of agreements for joint campaigns with other commercial subjects, where the counterparty may receive the personal data of their customers, the counterparty shall be bound to ensure compliance with the data protection legislation.

**Art. 38.** If, in the course of such joint campaigns, a data subject objects to the processing of his or her personal data and the subject is not party to an insurance and/or other type of commercial contract concluded with ZEAD BULSTRAD VIENA INSURANCE GROUP and has not provided a written consent for the processing of information related to him or her, the data shall be destroyed immediately on the grounds of expiry of the processing purpose.

**Art. 39.** Control over the observance of this policy shall be exercised by the Compliance Department.

### FINAL PROVISIONS

This Internal Policy has been adopted with Minutes 24/17.09.2018 of the Management Board of the company.