Pursuant to the 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 (hereinafter referred to as: the „GDPR“) and the provision of Article 24 of the Regulation, the Management Board of the company InterOmnia d.o.o., Zagreb, Ulica grada Vukovara 237 D, OIB (VAT No.): 26826437822, hereby adopts and publishes the following

# PERSONAL DATA PROTECTION RULEBOOK

## Preamble

Article 1

1.1 InterOmnia d.o.o., Zagreb, Ulica grada Vukovara 237 D, OIB (VAT No.): 26826437822 (hereinafter referred to as: the „Company“) is the data controller for processing of personal data of employees and third persons (hereinafter referred to as: “data subject” or “data subjects), whose personal data it processes in compliance with the principles and the provisions of the 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 (the General Data Protection Regulation, hereinafter referred to as: the “GDPR”), Act on the implementation of the General Data Protection Regulation and subordinate regulations, and the mentioned regulations apply directly to all issues not regulated by this Rulebook.

1.2 The Company shall, as the data controller, pursuant to Article 24 of the GDPR, appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. For the purposes of ensuring the implementation all measures, the Company enacts this Personal Data Protection Rulebook (hereinafter referred to as: the „Rulebook“) which is applicable as of 25 May, 2018.

1.3 The data subject entrusts his/her personal data for processing by having a contractual relationship with the Company, employment with the Company or use of the Company’s products and services, as well as indirectly, collected from other lawful sources. This Rulebook describes which data are collected by the Company, the manner in which it processes such data and for which purposes the data are used, as well as what rights of the data subjects are related to the processed data and other issues relevant for the protection and processing of personal data.

1.4 The terms used in this Rulebook, having gender meaning, regardless whether used in male or female gender, encompass equally both male and female gender. For the purposes of this Rulebook, the terms mean the following, equally as the terms used in the General Data Protection Regulation:

- “personal data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors

specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

- „processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- „the Company" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- „data processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- „recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

For the purposes of this Rulebook, other terms that were not expressly mentioned above, also have the meaning as the terms used in the General Data Protection Regulation.

1.5 At the moment of collection of personal data, the Company shall provide all information to the data subject, pursuant to the GDPR, particularly the provisions of Articles 13 and 14.

1.6 The Company may transfer personal data to a third country or international organisation, pursuant to the provisions of the Regulation.

1.7 The data subjects may send all requests directed at exercising the rights from the field of personal data protection in writing to the address of the Company or via e-mail to: gdpr@interomnia.hr.

**PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA**

Article 2

2.1 The Company, as the data controller, shall process the personal data fairly and lawfully. Personal data must be accurate, complete and up to date, and they may not be collected in the scope exceeding what is necessary for the established purposes. The personal data must 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.

2.2 The personal data relating to minors may be collected and further processed in accordance with the Personal Data Protection Regulation and by applying special protective measures prescribed by special laws.

**ORGANISATIONAL AND TECHNICAL _MEASURES FOR PERSONAL DATA PROTECTION**

Article 3

3.1 The Company implements appropriate technical and organisational measures to enable efficient application of data protection principles, such as minimisation of amount of data and inclusion of protection measures in the processing in order to fulfil the requirements from the Regulation and protect the rights of data subjects.

3.2 The Company shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3.3 The Company's professional and administrative employees who process personal data are obliged to undertake technical, human resources and organisational measures of personal data protection that are required to protect personal data from accidental loss or destruction, unauthorised access or alteration, unauthorised disclosure and any other misuse, and to establish the obligation of the persons employed in data processing.

3.4 The technical measures protecting data processing operations include at minimum physical access control, logical access control, security of operating systems and of e-mail accounts, use of antivirus software, access only through safe protocols and VPN channels and the use of data backup.

3.5 If the personal data processing is carried by another natural or legal person on behalf of the controller, the Company shall only use processors who sufficiently guarantee the implementation of appropriate technical and organisational measures in a way that the processing is compliant with GDPR requirements and that it enables protection of the data subjects' rights, which is regulated by contract or other legal enactment.

3.6 Personal data processed by the Company are given for use to other recipients exclusively based on the written request of the recipient, if required for conducting tasks within a legally established business activity of the recipient or the Company, i.e. if required for the purposes of fulfilling contractual and/or lawful obligations of the Company.

**DATA PROTECTION OFFICER**

Article 4

4.1 Pursuant to the provision of the GDPR, the Company has an appointed data protection officer, whose data are published on the Company's web site.

4.2 The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the

protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
(d) to cooperate with the supervisory authority;
(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

4.3 The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing

**LAWFULNESS OF PROCESSING**

Article 5

5.1 Personal data processing of the Company shall be lawful, based on at least one of the following legal bases:

a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to and/or after the entering into a contract;
c. processing is necessary for compliance with a legal obligation to which the controller is subject;
d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. The legitimate interests of the controller include, but are not limited to, the protection and improvement of business operations, increasing efficiency and protection of assets of the controller, the need to protect the network and personal data of employees and clients within the network from unauthorised access or data leaks, protection of personal data for which the Company is responsible as the Company of data, protection of security of its employees and other legitimate interests that the data subject was informed about pursuant to the provisions of GDPR.

5.2 The Company's processing of special categories of personal data mentioned in the GDPR is performed lawfully and in compliance with the provisions of GDPR, and on the grounds of at least one of the following legal grounds:

a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that

the data subject may not lift the prohibition from the paragraph on the processing special categories of personal data;

b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
e. processing relates to personal data which are manifestly made public by the data subject;;
f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 Article 9 of GDPR;
i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89, paragraph 1 based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

**TYPES OF PERSONAL DATA PROCESSED BY THE COMPANY**

Article 6

6.1 The Company processes the following personal data:

a) Basic identification data: name and surname, e-mail address;

b) Identification data: name and surname, personal identification number (so-called OIB), address of domicile, address of residence, date of birth, gender, nationality, contact data (e-mail address, telephone number), residence permits and place of work;
c) Data on employees' competencies: diploma, certificate, licence, professional expertise confirmation;
d) Financial data about the employees: type of contract, agreed salary, agreed fee, IBAN;
e) Record of working hours of employees: date of commencement of work, termination of employment, hours of field work, time of attendance at work place;
f) data related to data subjects' health (i.e. occupational disease, work injury, occupational disability, disability in general);
g) Other personal data, which the data subject or third person makes available when starting employment or during concluding and fulfilment of the contract, such as data from the personal ID card or other personal document, data involving children, bank account data, authorisation for signing or representation etc.

6.2 Personal data are collected either indirectly or directly from the data subjects orally and in writing.

**PURPOSE OF PROCESSING**

Article 7

7.1 The Company collects and processes the personal data for certain purposes including, but not limited to, the following:

- enabling and ensuring regular business operations
- provision of broker services, agency services and counselling related to insurance contracts
- conclusion and realization of insurance contracts
- applying data subjects for the purposes of exercising rights derived from pension and health insurance
- exercising rights and obligations deriving from employment or other contractual relationship for the data controller and data subjects
- achieving cooperation with outsourced associates
- exercising the rights of data subjects
- statistical purposes
- marketing purposes
- participation in tenders
- realization of communication with clients and potential clients and other data subjects

7.2 When introducing a new purpose of personal data processing or when altering the existing purpose of processing, the Company shall carry out, pursuant to Article 35 of GDPR, the an assessment of the impact on the protection of personal data and look into the implications for the system of processing itself and its safety. The new or altered purpose must be included in the Records of Processing Activities and this Rulebook and must be approved by the responsible person of the Company.

7.3 If the Company intends to additionally process personal data for the purpose different than the one the personal data were collected for, the data subject shall be provided with

information about that other purpose prior to such additional processing, as well as all other relevant information from Article 13, paragraph 2 of GDPR.

**PERIOD OF STORAGE**

Article 8

8.1 The Company in principle deletes personal data upon the end of contractual relationship or after the data subject requests the Company to delete data, and at the latest upon expiry of all legal, contractual and statutory obligations related to storing personal data, except in case the procedure of enforcement of unpaid claims or if a complaint was filed against a product or service within deadlines, all until the final end of the procedure regarding the complaint pursuant to current regulations.

8.2 The data subject's personal data shall be stored in a manner ensuring these are not automatically available, without the data subject's intervention, to an unlimited number of natural persons, namely locked in a cabinet, and if in electronic format of a dataset, on the computer of an employee which unlocks by entering employee password.

**RIGHTS OF THE DATA SUBJECT**

Article 9

The data subject is entitled to request from the Company – data controller access to personal data and rectification or erasure of personal data or restriction of processing concerning the data subject, or to object to processing of such data as well as the right to data portability in compliance with the provisions of GDPR. Where the processing is based on the data subject's consent, the data subject is entitled to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. The Company shall provide information on any conducted rectification or erasure of personal data or restriction of processing to each recipient to whom such personal data have been disclosed, unless such information proves impossible or involves a disproportionate effort. The Company informs the data subject on these recipients if the data subjects asks for it.

Article 10

10.1 The data subject shall have the right to obtain from the Company – data controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source;
(h) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
(i) appropriate safeguards relating to the transfer if the personal data are transferred to a third country or international organisation.

10.2 The Company shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Company may charge a reasonable fee based on administrative costs. The data subject makes the request for confirmation and access to personal data and information referred herein in writing (including electronic format). Where the data subject makes the request by electronic means, and unless requested otherwise by the data subject, the information shall be provided in a commonly used electronic form.

Article 11

Based on the request in written form (including electronic form), the data subject shall have the right to obtain from the Company – data controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement

Article 12

12.1 Based on the request in written form (including electronic form), the data subject shall have the right to obtain from the Company – data controller without undue delay the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
(c) the data subject objects to the processing of personal data concerning him or her and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes;
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or the Croatian law.

12.2 Where the controller has made the personal data public and is obliged pursuant to the above mentioned to erase the personal data, the Company, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical

measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

12.3 The provisions on data subject's right to erasure shall not apply to the extent that processing is necessary for exercising the right of freedom of expression and information, for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or reasons of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right of erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing or for the establishment, exercise or defence of legal claims.

Article 13

13.1 Based on the request in written form (including electronic form), the data subject shall have the right to obtain from the Company – data controller without undue delay the restriction of processing of personal data where one of the following grounds applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
(c) the Company no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
(d) the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

13.2 Where processing has been restricted under previous paragraph, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

13.3 A data subject who has obtained restriction of processing pursuant to this point shall be informed by the Company before the restriction of processing is lifted.

Article 14

Based on the request in written form (including electronic form), the data subject shall have the right, if this does not affect adversely the rights and freedoms of others, to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller, if the processing is based on consent or the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract and is performed by automated means. In exercising his or her right to data portability, the data subject shall have the right to

have the personal data transmitted directly from one controller to another, where technically feasible.

Article 15

15.1 The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party including profiling based on those provisions. The Company shall no longer process the personal data unless the Company demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. At the latest at the time of the first communication with the data subject, the Company shall explicitly bring to the attention of the data subject the right to object and shall presented it clearly and separately from any other information.

15.2 Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing, after which the personal data shall no longer be processed for such purposes.

**CONDUCT WHEN EXERCISING THE RIGHTS OF DATA SUBJECTS**

Article 16

At the latest within 30 days from when the request was filed, the Company shall provide each data subject at his or her request, i.e. request of his legal representatives or proxies, with all the requested information, and which may involve the following

1) the identity and the contact details of the controller and, where applicable, of the controller's representative;
2) the contact details of the data protection officer, where applicable;
3) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4) the categories of personal data being processed;
5) the recipients or categories of recipients of the personal data that were disclosed to them or shall be disclosed, if applicable;
6) the anticipated period for which the personal data will be stored;
7) the existence of the rights of the data subjects referred to in this Rulebook;
8) if the personal data are not collected from the data subjects, any available information as to their source;
9) if applicable, the fact that the Company tends to transfer personal data to a third country or international organisation, and the existence or absence of an adequacy decision by the Commission, or, in the case of transfers referred to in Article 46 or 47 or Article 49 paragraph 1 of the second sub-paragraph of GDPR, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

**RECORDS OF PROCESSING ACTIVITIES**

Article 17

If applicable pursuant to the provisions of the Regulation, the Company, shall maintain a written record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
(b) the purposes of the processing;
(c) a description of the categories of data subjects and of the categories of personal data;
(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;
(f) where possible, the envisaged time limits for erasure of the different categories of data;
(g) where possible, a general description of the technical and organisational security measures.

Article 18

18.1 In case of a personal data breach, the Company shall notify without undue delay to the supervisory authority about the personal data breach pursuant to the provisions of this Regulation not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

18.2 The Company shall document all personal data breaches, comprising the facts relating to the personal data breach, the consequences thereof and the remedial measures taken.

18.3 In case of the personal data breach that are likely to result in a high risk to the rights and freedoms of natural persons, the Company shall notify the data subject without undue delay on the personal data breach, pursuant to the provisions of the Regulation, unless if the Company has taken appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, or the Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise or it would involve disproportionate effort.

Article 19

The data subject is entitled to file a complaint to the competent supervisory authority if he/she deems that processing of personal data related to him/her violates the Regulation, as well as the rights to efficient legal remedies and other rights in compliance with the provisions of the Regulation.

Article 20

20.1 If some of the provisions of this Rulebook contradict to a provision of a subsequently enacted act or other regulation, this does not affect the validity of this Rulebook in whole; but, an appropriate provision of the act or other regulation shall apply directly instead of the provisions that are contrary to the act or some other regulation.

20.2 This Rulebook shall enter into force on 25 May, 2018.

Zagreb, 16 May 2018

Fudurić

INTEROMNIA d.o.o.
za posredovanje u
osiguranju i reosiguranju
Zagreb

InterOmnia d.o.o.

Paulina Fudurić, director