# PERSONAL DATA PROTECTION POLICY
# OF "INSURANCE COMPANY EUROINS" AD

**INFORMATION CARD**

| | |
|---|---|
| **Document approval date:**<br>**Date of entry into force:** | **30.01.2020**<br>**30.01.2020** |
| **Document version:**<br>**In effect from:** | **2.1**<br>**18.12.2020** |
| **Structure publisher of the document** | **"Methodology and Business Processes" Department** |
| **Term of validity of the document:** | **Perpetual** |
| **Approved by/on:**<br>**Amended by/on:** | **Management Board/30.01.2020**<br>**Board of Directors/18.12.2020** |

**CONTENTS:**

## CHAPTER I. GENERAL

**Art. 1.** (1) The "Insurance Company Euroins" AD ("IC Euroins" AD, the Company, the Administrator) is a legal entity with its registered office and administrative address in: Sofia 1592, district "Iskar", 43, Cristofer Columb" Blvd., and the main objects: insurance and insurance services.

(2) The Company is a personal data administrator within the meaning of Art. 4(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council dated 27 April 2016, concerning the protection of individuals with respect to personal data processing and of the free movement of such data, and for the repeal of Directive 95/46/EC (General Data Protection Regulation, GDPR).

(3) The Company, being a personal data administrator, abides by, announces, and provides information to the data subjects within the meaning of Art. 13 and Art. 14 of the GDPR through a Privacy Notice, in relation to the provision of insurance services, a Privacy Notice to the employees and persons employed under a provisional contract, the Policy for Confidentiality and Protection of the personal data, processed by the "IC Euroins" AD in its capacity of personal data administrator when selecting the staff, and the Rules for providing information on the exercise of the rights of the personal data subjects.

(3) The Company, as a personal data administrator, determines:

1. the type of the processed data, pursuant to the intended objectives;
2. the purpose and means of processing;
3. the measures to ensure security of the personal data, abiding by the requirements of the GDPR, the Personal Data Protection Act (PDPA), and other regulatory acts.

**Art. 2.**(1) This policy has as its objective to regulate:

1. the keeping, maintenance and protection of the registers with personal data (the personal data processed by the Company);
2. the obligation of the persons authorised to process personal data, and their responsibility;
3. the required technical and organisational measures for protection of the personal data from unauthorised processing (unauthorised destruction, loss, change, not authorised disclosure or access to the personal data of third parties, as well as any other illegal forms of personal data processing).

(2) The policy is applied for personal data processed by the Company.

(3) The Company processes personal data in compliance with the following main principles:

1. legitimacy, good faith, and transparency;
2. limitation of the objectives;
3. reducing the data to a minimum;
4. precision;
5. storage restriction;
6. integrity and confidentiality.

(4) The Company bears the responsibility of being in a position in every single moment, to demonstrate the compliance with the principles related to personal data processing (accountability principle).

(5) The Company processes personal data on its own, assigning it in writing to the individual processing the personal data, or as joint administrator (according to Art. 26 of the GDPR).

## CHAPTER II. PURPOSE AND KEEPING OF THE REGISTERS

**Art. 3.**(1) The Company structures, organises, maintains and updates the personal data registers, by independently setting the objectives and means for data processing.

(2) The registers are kept in writing and in an electronic format. The data carriers are stored in the designated premises with regulated access.

**Art. 4.**(1) The hard copies of personal data are stored in folders (files) in a manner not permitting their integrity to be disturbed, or information with statutory protection to be lost.

(2) Only authorised employees of the Company have access to the respective files, in compliance with the job descriptions and the functional characteristics, and with direct orders by the Chairman of the Board of Directors (BD), or the executive directors. The possibility of providing access for other people to the personal data in its processing is limited and expressly specified in this policy, in other written documents of the Company, or in the regulatory framework.

**Art. 5.**(1) The processing of personal data in an electronic format, is carried out only in the corporate network, not connected with the public network, with the rights for access and processing of personal

data within the systems being determined and provided adhering to the official commitments and observing the conditions and procedure set out in the Access Control Rules. Software products for data processing, adapted to the specific needs of the Company, are used when working with the data.
(2) Only the authorised persons have access to the operating systems, where personal data is processed, through username and password for authentication. The protection of the electronic data from unauthorised access, damage, loss or destruction, is ensured by maintaining firewalls, antivirus programs, renovation of operating systems, periodic data archiving, periodic change of passwords, VPN, and also by keeping the information on hard copies.

## CHAPTER III. PERSONAL DATA STORED IN THE REGISTERS

**Art. 6.**(1) In the human resources register is collected and stored the personal data of candidates for employment, the persons hired by permanent or provisional employment contracts and third parties related to such persons, when such data is required to implement the legislation (family members, persons that are in economic or other normatively regulated connection) in respect of the administration of the processes, related to the obligations of the Company in terms of labour, tax and social security legislation, and special legislation, relevant to the activities, with the purpose of:

1. staffing;
2. individualisation of the parties under permanent or provisional employment;
3. fulfilment of the regulatory requirements of the Labour Code, the Social Security Code, the Health Insurance Act, the Personal Income Tax Act, the Accountancy Act, the Obligations and Contracts Act, the Insurance Code, and others;
4. the preparation of documents any kind for all activities related to the existence, modification or termination of the permanent or provisional employment relationships, to the persons in this regard (contracts, additional agreements, documents certifying the length of service, official notices, information sheets, certificates or similar), procedures in connection with the requirements for qualification and reliability, and procedures in connection with the requirements towards the employers for the securing of self and healthy working conditions, etc.;
5. correspondence with a supervisory body or other regulations specific for the activity.
6. establishing a contact with the person by phone, sending correspondence to a physical or electronic address, concerning the administration and fulfilment of permanent or provisional employment contracts, to which the data subject is a party;
7. bookkeeping, reporting the remuneration to the above persons under permanent or provisional employment contracts;
8. other according to what is stated in the Privacy Notice about the employees and the persons employed under provisional relationship, and the Policy for Confidentiality of the personal data, processed by "IC Euroins" AD, in its capacity of personal data administrator in selecting the staff.

(2) The personal data of the Company employees is arranged in personal employment files, and is stored in a file cabinet. They are located in a specially equipped room, intended for work of the authorised employee(s), engaged in the activities of human relations management.
(3) Access to the information of the personnel files, stored by automated means, is available to authorised employee(s), as set forth in paragraph 2, second sentence, through the password for opening such files. The possibility of providing access for another individual to the personal data when it is processed, is limited and expressly regulated in this policy and the relevant internal rules of the Company, as long as it does not ensue from the current legislation.
(4) In the register are processed the following categories and types of data:

1. Identification information (physical identity) – the full name, Personal ID No., card of identity No., date and place of issue, place of birth.
2. Contact information/information on the positioning – phone numbers for contact, email address, permanent/present address, or address for correspondence.
3. Economic identity – data on the bank account for remuneration transfer, data on the property status and the economic relatedness, according to the Code of Insurance (CI).
4. Social identity – education status and length of service, a document for acquired education, qualification, or legal capacity, when such is required for the position about which a person applies, etc., labour activity documents and professional biography, documents certifying kinship ties or marital status (marriage certificate, child's birth certificate, declarations on the existence of kinship ties), data related

to court sentences or violations – criminal record certificate, when required to get a job, declarations for qualification and reliability.

5. Special categories of personal data (health identity) – data on the state of health of a person, contained in a health certificate to start work, appraisals by the medical expert report bodies with respect to the submission of documents on temporary incapacity for work and permanently reduced capacity for work, data on religions other than Orthodox Christianity, when declared by the person for enjoyment of the rights set forth in Art. 173 of the Labour Code.

(5) The data for this register is collected upon recruitment/assignment of work under permanent or provisional employment relationship of a person in fulfilment of a regulatory obligation – the provisions of the Labour Code, the Social Security Code, the Health Insurance Act, the Personal Income Tax Act, the Accountancy Act, the Obligations and Contracts Act, the Insurance Code, and others, in one of the following ways:

1. Oral interview with the person (upon starting work, or in the process of work).
2. On paper – written documents – petitions, applications for employment/for execution of work under permanent or provisional employment relationship, and the enclosed documents, for modification or termination of such relationship, on current matters in the process of work, filed by the person.
3. From external sources (from judicial, financial, social security, taxation and other institutions, in compliance with regulatory requirements).
4. In every case when it is necessary, based on a regulatory requirement, the persons whose data is obligatorily subject to processing in the register, submit the required personal data to the administrator, respectively to the authorised empoyee.

(6) The employee from the "Human Resources" Department has the obligation to make available to the data subject the information under Article 13 of the GDPR on a special form, not later than the moment of receiving the data thereto.

(7) In certain cases limited access to personal data of that register may be granted to: the members of the Board of Directors of "IC Euroins" AD, the chief accountant as well as the persons performing technical accounting operations in preparing the payment documents related to transfers of salaries by banks, as well as other employees of the Company, who have to process personal data in view of the fulfilment of their duties according to their job description, including but not limited to, legal experts.

(8) The authorised empoyee under para. 2, second sentence, provides access to the information kept by him/her, in compliance with the requirements of this policy and, as regards the unresolved cases, following an order in writing by the Chairman of the Board of Directors, or by an executive director.

(9) The personal data collected upon staff recruitment, is processed and stored according to the Policy for Confidentiality and Protection of the personal data, processed by "IC Euroins" AD, in its capacity of personal data administrator, when selecting the staff.

**Art. 7.** (1) In the register, regarding the clients of the Company – users of insurance services and intermediaries, is collected and stored personal data of contracting parties, intermediaries and users of insurance services, in view of:

1. the insurance goals;
2. individualisation of the persons for the respective type of insurance;
3. compliance with the regulatory requirements under the Insurance Code, and other;
4. the tariffing;
5. in all activities related to the preparation of any documents and information sheets for the persons (testimonial letters, certificates, assurance letters, and similar);
6. establishing a contact with the person by phone, to send correspondence concerning the execution of the respective contract;
7. other according to what stated in the Privacy Notice, in relation to the provision of insurance services.

(2) The employees who are directly involved in the activities for entry into and administration of insurance and mediation contracts, are obliged to make available to the data subjects the information under Art. 13 of the GDPR in the form of the Privacy Notice, validated and published on the official internet website of the Company with respect to the provision of insurance services.

(3) The hard copies of personal data are stored in document pockets, folders, file cases, cabinets, metal cases and similar instruments for the organisation, arrangement and storage of documents. In

the service rooms where the data is processed, such as parts of buildings or separate wings of floors, the physical access is monitored, intended for work of the authorised empoyees of the Company, who have the obligation to process the personal data media and other information protected by the law, according to their job description.

(4) In the keeping the register of an electronic medium, the personal data is entered and processed in the corporate networks and the software programmes with access control.

(5) The following data types are supported:

1. Identification information (physical identity) – forename, patronymic and surname, Personal ID No., data from the identity document.
2. Contact information/information on the location – e-mail, address and telephone number.
3. Economic identity – bank account number, data on the property status (owned property, such as information on a road vehicle, real estate), history of the payments.
4. Social identity – length of service, professional experience, profession, remuneration.
5. Special categories of personal data (health identity) – information concerning the health status of the insurance services users (diagnosis, epicrises, other medical documents about performed tests, examinations, or other interventions).

(6) The personal data in the register under Art. 7 is collected following the entry into the relevant type of contract, filing a claim/registration of a damage, complaint, etc., by individuals, about whom the data refers (the insured persons, respectively the insuring and/or the injured persons, respectively their proxies), governmental bodies and third parties, according to the CI and from public registers.

**Art. 8.**(1) In the register, with respect to the records and archives offices of the Company, is gathered and stored personal data about various categories of individuals – insurance services users, intermediaries, suppliers, legal representatives and proxies, including data made available in connection with the establishing and exercising of legal claims before judicial and extrajudicial instances, and data processed by means of inquiries of regulatory and supervisory bodies.

(2) The data in the register under Art. 8, para. 1 is collected and processed with the purpose of conducting the management of records and archival storage of paper documents, in keeping with the internal rules, procedures, instructions and directions of the Company.

(3) Archiving and storage of documents is carried out in accordance with the Rules on archival activity, the Directions for application of the nomenclature of cases, and the Nomenclature of cases with deadlines for storage of the cases.

(4) The following categories of personal data are processed in the register under Art. 8, para. 1:

1. Identification information (physical identity) - names, Personal ID No./Foreigner's Personal No., data from the identity documents.
2. Contact information/information on the location – e-mail, address and telephone number.
3. Other data – provided at the discretion of the individual, author of the initiating document, deposited in the record keeping system of the Company.

**Art. 9.**(1) The Company may process personal data wholly or partially with automatic devices in registers with personal data for purposes stemming from the legitimate interests of the Administrator or a third party, in the context of the management of the physical safety, property protection, access control, monitoring of the employees for the purposes of implementing the official duties and the use of resources and information, information technology security, network security and enhancement of the customer service. In the Company is processed personal data of persons hired under permanent or other employment relationships and of third parties, passing through a guarded perimeter, calling the telephone exchange of the Company, visiting the buildings/offices of "IC Euroins" AD, having access on legitimate grounds to information resources, or using resources about which are used security and surveillance systems. It is done through access cards, video surveillance systems, GPS- systems of the company cars, and monitoring of the company information resources. The data is collected in the course of the application of the relevant technical and organisational measures for protection, with a view to prevent unauthorised access to buildings, premises and facilities and systems, where personal data related to the "IC Euroins" AD activities is processed.

(2) In the register under Art. 9, para. 1 are processed the following categories of personal data:

1. Identification information (physical identity) – employee's full name, service card number, official e-mail address, position, logs, photograph or video, showing the persons shot within the scope, recording of telephone conversation, conducted by calling from or to a telephone exchange of the

Company.
2. Information on the situation – geographical location;
3. Online identifiers – passwords, user name, IP address of the device used, device information when using VPN.

## CHAPTER IV. ASSESSMENT OF IMPACT, AND TECHNICAL AND ORGANISATIONAL MEASURES FOR PROTECTION OF THE PERSONAL DATA

**Art. 10.**(1) The Company employees are acquainted as soon as they are employed, and subsequently also periodically, but not less frequently than once a year, with the requirements of the current legislation, regulating the protection of the personal data, as well as with this policy.
(2) The Company employees to whom, due to the nature of the work performed, and/or to the position held, is assigned the task to process personal data, are obliged in their actions to observe the compliance with the legislation, regulating the protection of the personal data. At a failure to observe such obligation, they bear responsibility pursuant to the Bulgarian legislation.
**Art. 11.**(1) The Company determines or appoints an official on data protection (ODP), of whom it duly informs the supervisory body for protection of the personal data and the data subjects. Contact with such person is carried out through the e-mail address dpo@euroins.bg or office@euroins.bg.
(2) Functions of the ODP:
1. The ODP participates in an appropriate manner and in due time in resolving all issues related to the protection of the personal data, including but not limited to, when decisions are made, having an impact on the data protection (adoption and modification of new in-house policies, rules and procedures, introduction of new software and business products), and also when a violation of the data security or other incident is ascertained.
2. The ODP acts as a person for contact with the supervisory body and the data subjects, and the latter may address the ODP on any matters related to the processing of their personal data and to the exercise of their rights, according to the GDPR.
3. The ODP informs and advises the Administrator and the employees who perform the processing of personal data, about their obligations for adherence to the data protection legislation, the internal rules of the Company, takes part in the activities on raising the staff awareness, including on the organisation and conducting of training courses on topics related to the processing and protection of the data safety.
4. The ODP monitors the observance of the legislation and of the internal rules of the Company on data protection, collecting information to determine the processing activities, analyses and checks their performance, and makes recommendations to the Administrator.
5. They express their opinion on the necessity of conducting an assessment of the impact on the data protection (AIDP) for a particular type of processing, what methodology to be used for its implementation, what guarantees to be applied to reduce the risks for the rights and interests of the data subjects, whether the AIDP was made correctly and whether the conclusions lead to the necessity of a preliminary consultation with the supervisory body.
6. They keep a register of the activities of processing according to Art. 30 of the GDPR, an Operational Register of requests for exercise of rights, a Register of the data security violations.
7. Other activities according to their job description.
(3) The ODP is independent and the Administrator provides to them technical, organisational, training, financial and any other assistance as well as access to the respective registers and operations, to the extent necessary with regard to the fulfilment of their obligations.
(4) The ODP keeps confidentiality and secrecy in the performance of their tasks, ensuing from this policy and from the applicable legislation.
**Art. 12.** In the register of the processing activities according to Art. 30 of the GDPR is described the processing of personal data in the data registers of the Company.
**Art. 13.**(1) The personal data in the supported registers is stored and protected from accidental or illegal destruction, from accidental loss, unauthorised access, modification or disclosure as well as from other wrongful forms of processing, through a system of technical and organisational measures.
(1) The protection of the personal data can be:
1. physical;
2. personal;

3. documental;
4. protection of automated information systems and/or networks;
5. cryptographic protection.

(3) The measures for personal data protection are conformed to the contemporary technical progress achievements, the application costs and the nature, range, context and objectives of processing, as well as to the hazards with different probability and weight for the rights and liberties of the individuals, and when appropriate, the measures set forth in Art. 32 от GDPR are applied.

(4) The technical and organisational measures, which the Company applies for the single registers and activities of processing, are entered in the register of activities of processing, according to Art. 30 of the GDPR. The measures are updated and are subject to periodic survey in case of changes in the objectives, means and grounds for processing, as well as at the suggestion of the units (departments/directorates) participating in the processes of personal data handling, recommendations from audits and verifications, or at the suggestion of the ODP.

(5) The physical protection measures comprise rules, procedures and directions from the Management Board of the Company, to forestall unauthorised access to buildings, premises and facilities, where personal data is processed, such as: controlled regime of entry, movement and exit from the work premises; safe-keeping of keys for rooms, cases, cabinets or other facilities, serving to store information which contains personal data, fire-fighting systems, regulated regime of visits, or other

(6) The personal protection includes a system of organisational measures, providing a suitable level of knowledge of the regulatory framework in the field of the personal data protection, obligations not to divulge critical information among the staff or outside the Company, holding training courses, practices of the employees for response in case of crises, including events which threaten the data security.

(7) The documentary protection is a system of organisational measures, which consists in the regulation with procedures and rules of the activities involved in the personal data processing, and also the keeping of activity registers, of an Operational Register of requests for the exercise of rights, procedures for safe-keeping, access and destruction of data carriers, determining periods for storage.

(8) The Company applies a system of technical and organisational measures in the processing of data by means of information systems, with the purpose of protecting from illegal forms of personal data processing, which guarantees a clear distribution of roles and responsibilities, identification and authentication, control of the session and of the remote accesses, antivirus protection, keeping spare copies for recovery. The application of the protection measures is ensured by the Information security policy and a system of procedures and rules for control of the access to the information systems, changes, configuration of the antivirus system, and other. The department of "Information Services, Statistics and Analyses" performs an ongoing analysis of the capability of the network and the information systems to withstand the high level of casual events, wrongful or ill-intentioned actions, which could have a sizeable impact on the integrity, existence and confidentiality of the data preserved in and transmitted to the Company, and offer changes whenever needed, in line with the levels of risk.

(9) Cryptographic protection is a system of technical and organisational measures, which are applied in order to protect the personal data from unauthorised access in transmitting, divulging or providing. The principal cryptographic protection measures are:

1. the standard cryptographic capabilities of the operating systems;
2. the standard cryptographic capabilities of the database management systems;
3. the standard cryptographic capabilities of the communication equipment;
4. systems for distribution and management the cryptographic keys;
5. the electronic signature systems defined by the regulations.

**Art. 14.** (1) The AIDP is a process aiming to describe the processing of personal data, to evaluate its necessity and proportionality, and to help for the management of the risks for the rights and liberties of the individuals, appraising them and defining measures of coping with such risks.

(2) Making the AIDP is obligatory for an operation or a set of operations, where there is a probability for the processing to pose a high risk to the rights and liberties of the individuals as well as to operations that are included in a list of the supervisory body as per 35(4) of the GDPR. The Administrator justifies and documents the reasons, because of which he/she makes a decision whether to carry out the AIDP or not, requesting also the opinion of the ODP. When the processing is carried out wholly or partially by an employee who processes personal data, such employee assists the Administrator in the performance of the AIDP in compliance with the requirements of the GDPR, taking into account the

nature of processing and the information to which access has been provided. The role and the responsibilities of the employee who processes personal data with respect to the AIDP, are defined in the concluded contract.
(3) The units (departments/directorates) responsible for the processes of personal data processing, determine the objectives and means for processing and/or assessment of the risk, as well as the ODP, may propose for the AIDP to be carried out. They provide the necessary information for the AIDP and participate in the process of its documentation and validation.
(4) When performing the AIDP a suitable methodology is used, whose content is in conformity with the announced guidelines, recommendations and best practices of the competent data protection authorities on data protection (supervisory body and the European Data Protection Board, respectively the Working Group for the Protection of the Individuals in the processing of personal data as set forth in Art. 29).
**Art. 15.**(1) Personal data is stored until the goals for which it was collected have been achieved, and pursuant to the deadlines set for storage of the respective medium.
(2) Storage and destruction of carriers of personal data is performed according to the Rules for archival activity; the Nomenclature of the cases with deadlines for their storage; the Procedure for the transfer of documents to the archives; the Procedure for destruction of documents, all adopted by the Company.

## CHAPTER V. RIGHTS OF THE DATA SUBJECTS AND PROCEDURE FOR EXERCISING THEM

**Art. 16.**(1) The personal data subjects may exercise their rights set out in Art. 15 – 22 of the GDPR, by filing a written application to the Administrator. The application may be filed:
1. in electronic way, signed with an advanced electronic signature, based on a qualified certificate for electronic signatures, or a qualified electronic signature, as set out in the Rules for the providing of information on exercising the rights of the personal data subjects;
2. on the spot in an office of "IC Euroins" AD by the data subject. Provided that the request is submitted by an authorised representative, the original power of attorney is presented for verification;
3. by post to the address of the Company Headoffice (43, Hristofor Kolumb Blvd., Sofia);
4. and is free of charge.

(2) When the claims of the data subject are obviously unfounded or excessive, in particular due to their repetitiveness, the Administrator may charge a reasonable fee, or refuse to take action on the request.
**Art. 17.** The application contains the name of the data subject and other data, which enable the Administrator to identify the data subject as an identification number (Personal ID No.), number of insurance policy/contract, etc., description of the request, preferred form of delivery when access to personal data is requested, and correspondence address. The application is registered in the common incoming register of the Company and in the Operational Register of requests for exercise of rights of the data subjects, supported by the ODP.
**Art. 18.** Access to the subject's data is provided in the form of:
1. oral explanation;
2. written explanation;
3. review of the data by the person himself (herself) or their proxy;
4. delivery of a copy of the requested information.

**Art. 19.**(1) When a request is filed by a data subject according to Art. 16, the application is submitted to the ODP for review and preparation of a motivated draft decision. The units where personal data is processed, lend support in the course of the examination of the application, providing access to data carriers and assistance when the Administrator must undertake specific actions with respect to the exercise of the rights of the data subject.
(2) The deadline for examination of the application and pronouncement on it is one month from receipt of the request. Such deadline may be extended by another two months, taking into consideration the complexity and number of requests. The Administrator informs the data subject about any such extension of the deadline within a month from receiving the request, stating the reasons for the delay as well.
(3) The decision is notified in writing to the applicant, is received in person with a signature affixed by the addressee, or by post with acknowledgement of receipt. When a data subject files a request by

electronic means, the information is possibly delivered by electronic means, unless the data subject has stated otherwise.
(4) When the data does not exist, or cannot be delivered on a specific legal basis, the applicant is denied access to it by a motivated decision. The refusal to grant access may be appealed against by the individual before the authority stated in the letter, and within the specified period.
**Art. 20.** The Company announces the terms and conditions for the exercise of the rights of the data subjects, according to the GDPR on its official internet website in the Rules for providing information on the exercise of the rights of the personal data subjects.

## CHAPTER VI. RESPONSIBILITY AND CONTROL

**Art. 21.**(1) Ongoing control of the compliance with this policy is conducted by the heads of the respective units of the Company's structure (directorates/departments).
(2) Subsequent control of the observance of the requirements for legitimate and conscientious personal data processing is carried out by the specialised service "Internal Control".
(3) The ODP informs the Board of Directors at least once a year with a report on its activities, including the number and type of requests filed for the exercise of the data subjects' rights, the participation in procedures for coordination of documents, the AIDP and in case of need, proposes concrete measures in connection with the observance of the applicable legislation on personal data protection.
(4) The Board of Directors conducts periodically, but not less than once a year, a survey of this policy and of the relevant internal documents, which introduce rules, policies and principles of legitimate and scrupulous processing of personal data, updating them if necessary.

## TRANSITIONAL AND FINAL PROVISIONS

**§1.** For the purposes of this policy the notions used have the meanings given them by the GDPR and the PDPA.
**§2.** This policy is subject to disclosure and to be made available to all employees of the Company through a shared resource in the internal corporate network, for information and execution.
**§3**. This policy was adopted by the Management Board (MB) of "IC Euroins" AD on 30.01.2020, it took effect on the same date, and supersedes the Instructions on the conditions and ways of collecting, processing, storing and protecting the personal data, approved by a decision of the MB of the Company made on 15.08.2017. The policy was revised by a decision of the MB of the Company from 18.12.2020, and the changes took effect on the same date.