Personal Data

PERSONAL DATA PROTECTION POLICY

The société anonyme under the corporate name "**NEQUS REPRESENTATION OF INSURANCE AND REINSURANCE COMPANIES SOCIÉTÉ ANONYME**" and the distinctive title "NEQUS REP S.A." having its registered office in Nea Smyrni, Attica, at 171 Syngrou Avenue, with T.I.N. 800562232, Tax Office for S.A. Companies of Piraeus and legally represented, hereinafter referred to as "the Company", in the framework of its activity and statutory purposes, shall keep personal data as the Controller and take all appropriate technical and organizational measures for its compliance with the national and European legislation related to the protection of individuals with regard to the processing of personal data relating to them, hereinafter referred to as "data", in particular with the Regulation (EU) 2016/679 (General Regulation on Data Protection), hereinafter the "Regulation", on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The following constitute our policy in the framework of the above compliance and in particular:

1. The general principles followed when processing personal data.
2. Type of data that may be processed by our company.
3. The purposes of processing.
4. Kind of recipients, to whom the data may be disclosed
5. Transfer of data to third countries.
6. Time period for which the data is kept and what happens when such period passes.
7. Rights of data subjects.
8. The obligations of the Company during the data processing.
9. Installation of Closed Circuit Television equipment for security reasons.
10. Update - amendment of our Policy.

1. General principles of Personal Data processing.

The Company shall ensure that the processing of data is carried out in accordance with the general principles provided by law and in particular shall ensure that:

· The collection is always carried out fairly and lawfully, for a specified, explicit and legitimate purpose.

· The processing is carried out with the consent of the subject to the rights, provided that he/she has been previously informed in detail on everything he/she is entitled to know, as well as on his/her rights, including the main right of free revocation, at any time, unless otherwise provided by law.

· Any data processing is carried out in a lawful manner, in compliance either with the relevant prior consent of the subject, if processing is based on it, or according to the legal ground allowing the respective processing.

· The data is relevant to the purpose of the processing, adequate, accurate and not excessive in relation to the respective purpose.

· The data is regularly updated or supplemented, so that they always comply with the above.

· The data is kept for the minimum required time, always based on the purpose of their processing.

· It observes at all times the appropriate security measures for ensuring the security and integrity of the data from any danger, unauthorized access, loss, damage, illegal use, etc.

More specifically on the subject's consent, we shall point out that according to the law, the latter is not required:

(a) when processing is carried out for the performance of a contract into which the subject has entered with us or in order to satisfy his/her request;

(b) when processing is carried out for the Company's compliance with its legal obligations;

(c) when processing is carried out to protect the vital interests of the subject;

(d) when processing is carried out for the performance of a task in the public interest and

(e) when processing is necessary for the purposes of the legitimate interests pursued by our Company, unless the interest or the fundamental rights and freedoms of the subjects prevail over those interests.
Minors' data shall be kept by the Company only if they have been provided by those who exercise parental responsibility and only for the purposes of fulfilling a relevant contractual relationship for the minor's benefit. The Company shall in no case deal directly with minors.

2. Type of data that may be processed by our company.
The Company shall process the personal data that are absolutely necessary for the respective purpose of processing. We have implemented procedures to check their accuracy, along with the obligation of the subjects to inform the Company in a timely manner on any change.

More specifically, the data processing by the Company shall include the following categories:

a. Identification Data e.g. first name, last name, date of birth, police ID/passport number, S.S.N., T.I.N.

b. Contact Data e.g. email/mail address, phone/fax numbers.

c. Payment Data e.g. bank accounts, debit/credit and other bank cards.

d. Insurance Data, i.e. data necessary for the management of an insurance contract, (e.g. health data, driving history etc.).

e. Settlement Data, i.e. data necessary for the management of insurance claims included in the application for compensation/redemption/payment of insurance indemnity or in accompanying documents/supporting documents or related to such indemnity.
The personal data processed by the Company shall be kept in written form and/or by electronic and magnetic means.

3. The purposes of processing.
The Company may process personal data for the following purposes:

a. administration of an insurance policy during its term or after its expiration, including the assessment, control and settlement of the insurance compensation in the event of occurrence of an insurance risk or the payment of the amount stipulated in the terms of the policy (insurance indemnity),

b. compliance of the Company with obligations imposed by the current legal and regulatory framework and avoidance of insurance fraud,

c. research that the Company may need to carry out in relation to other, past or future, applications of the policyholder/insured and/or beneficiary of insurance compensation.

4. Kind of recipients, to whom the data may be disclosed

Data may be transferred:

a. to insurance or reinsurance companies upon lawful request,

b. to public/judicial authorities,

c. to the Insurance Companies Statistical Service (I.C.S.S. archive) of the Hellenic Association of Insurance Companies,

d. to providers cooperating with the Company in the framework of its lawful operation, such as insurance intermediaries, file storage and management companies, assistance services companies, customer service call centers, lawyers, doctors, researchers or experts.

5. Transfer of data to third countries.

If the Company needs to transfer data outside Greece or outside the EU, this will take place under the conditions of Articles 44 et seq. of G.D.P.R. EE 679/2016. In any case, the transfer of personal data to countries outside the European Economic Area (EEA) shall take place only if these countries provide an adequate level of protection of the personal data.

In the event that a third country outside the European Union (EEA) does not provide an adequate level of personal data protection, the personal data will only be transferred to that country, only if data protection is provided for in a data transfer agreement ensuring an adequate level of protection or meeting the conditions explicitly provided for in the European and national legislation (e.g. the data subject has explicitly consented to the transfer). The Company shall ensure with the appropriate procedures that the required procedures are implemented by the local competent Authorities.

6. Time period for which the data is kept and what happens when such period passes.

The Company will collect, store and generally process data for a period of up to twenty (20) years after the end of the year in which they were collected, if there is a legal dispute, and up to five (5) years in case no legal dispute exists, unless a legal dispute is pending beyond the above processing time and until its termination according to an irrevocable court decision.

In other cases, the time of data retention will be the one provided by law, the granted consent of the subject and the legitimate interests of the Company, provided that the rights of the subjects do not prevail.

In case the retention period of your data expires, the Company shall pay special attention to their destruction. In particular, it has established and implements a relevant procedure for this purpose after examining that the maintenance of archival material is not required to comply

with legal and regulatory requirements or to protect the interests of the Company, based on the instructions of the Hellenic Data Protection Authority. The Company shall ensure that the above process of destruction of files containing personal data also binds third parties that provide services in the name and on behalf of it and any other persons with whom it cooperates in the framework of outsourcing contracts or other types of agreements.

7. Rights of data subjects.

Each subject is entitled to exercise on a case-by-case basis the rights provided by the General Regulation of Personal Data (EU 679/2016) and the applicable national legislation, under the conditions set out in this regard.

More specifically:
· He/She has the right to access his/her personal data.
· He/She has the right to request the correction of inaccurate or out-of-date data relating to him/her or the completion of incomplete data relating to him/her.
· He/She has the right to request the deletion of his/her data from the Company's files, provided that their processing is not necessary for the pursuit of the purposes for which they were collected and it is not justified by any other lawful cause.
· He/She has the right to request the restriction of the use of his/her data in case of questioning their accuracy.
· He/She has the right to receive the data he/she has provided in a structured, commonly used format.

The exercise of the above rights presupposes the submission, without any cost, of a written application to the Company. For any issue he/she may contact the data Controller of the Company (Mr. Zirganos Efstathios, son of Athanasios, 6 Agiou Konstantinou St., Athens, P.C. 10431, email dpo@nequsrep.com). In any case, he/she has the right to contact the Hellenic Data Protection Authority, either in writing (1-3 Kifissias Ave., P.C. 115-23), or electronically (www.dpa.gr).

In case of exercise of one of the above rights, the Company will take every possible measure for his/her satisfaction within thirty (30) calendar days from the receipt of the relevant application, informing in writing of his/her satisfaction, or the reasons that prevent the exercise.

8. The obligations of the Company during the data processing.

The Company is obliged to apply and shall implement all the requirements of the legal framework for data protection.

Particular emphasis is placed on, inter alia, the following:
· **Ensuring Privacy and Processing Security:** The processing of personal data is confidential and is carried out exclusively by persons under the control of the Company. These persons are selected on the basis of strict criteria, which aim to provide adequate guarantees in terms of knowledge and personal commitments to maintain confidentiality. In addition, audits are carried out on a regular basis in order to strictly apply the criteria and implement the procedures established by the Company for this purpose. The Company shall take all appropriate organizational and technical measures to secure the data and protect them from breaches, such as accidental or unlawful destruction, accidental loss, alteration,

prohibited transfer or access and any other form of unlawful processing. The measures taken shall always aim to ensure a level of security commensurate with the risks involved in the processing and the nature of the data being processed.

· **Information Systems Security:** In order to ensure the confidentiality of all information kept in its information systems, the Company has established appropriate measures for the security of information systems, which achieve the protection of data transferred through the data and voice networks used by the Company, effectively control the access of users to its information systems and ensure the protection of the information that these systems manage, while incidents of breach of security of the Company's information systems are detected in a timely manner and, as far as possible, are prevented.

9. Installation of Closed Circuit Television for security reasons.

In order to prevent the theft of goods and criminal acts and ensure the safety of staff, the Company shall install closed circuit television equipment in its facilities, where this is deemed necessary. The installation and operation of these systems is in accordance with the requirements of the current regulatory framework.

10. Update - amendment of our Policy.

The Company may update, supplement and/or amend this Policy in accordance with the applicable legal framework. In this case, the updated Policy will be posted on the Company's website, to which we refer each operator, in order for him/her to always be informed.