CODE OF CONDUCT AND PERSONAL DATA (GDPR)
SECURITY POLICIES

Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

Version: 1
Issue date: 24/05/2018

GENERAL TOURISM AND PUBLIC RELATIONS COMPANY "T&T EXECUTIVE SA"

The registered office of the Company is located at 192, KIFISSIAS AVENUE & 24, IEREOS DOUSSI STREET, AMAROUSSIO 15124, GREECE. The Company is registered with the Athens Corporation Tax Office (FAE Athens) with TIN 094438218.

The Company as a legal entity:

Indicates and declares the following as regards the preparation and generation of this Code of Conduct and Personal Data Security Policies:

1. DEFINITIONS

1.1. T&T EXECUTIVE AE has been active in the provision of travel services (airline reservations, car rentals, hotel room reservations) and conference and event organisation services to both private and corporate clients, since 1996.

1.2. **Personal Data**
'Personal data' means any information relating to an identified or identifiable natural person. This includes both ordinary personal information (e.g. information such as the name, age, marital status, residence address, e-mail address, bank account details, IP address, phone/fax numbers, payment details (i.e. bank account numbers, debit/credit and others bank card numbers), ID card or passport number, TIN, SSRN (AMKA), education and profession details, place of birth, insurance details and any other information necessary to conclude contracts and manage the services provided by the Company, namely the provision of travel and event arrangement services to its clients.

1.3. **Data subject**
'Data subject' means he natural person which is the subject of such data.

1.4. **Processing**
'Processing' means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as the collection, recording, organisation, structuring, storage, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion or destruction of such data.

1.5. **Controller**
'Controller' means the natural or legal person which, alone or jointly with others, determines the purposes and means for processing such personal data.

1.6. **Third Party**
'Third party' means any natural or legal person, other than the controller and those under his/her direct authority, authorised to process personal data.

1.7. **Data Files or Filing System**
'Data files or filing system' means any structured data set accessible according to specific criteria.

1.8. **Consent**
'Consent' means any freely given, specific, informed and unambiguous indication by which the data subject signifies his/her agreement to the processing of personal data relating to him or her.

1.9. **Profiling**
‘Profiling’ means any form of processing of personal data to evaluate certain personal aspects relating to a data subject for the purpose of analysing that data subject's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour or movements.

1.10. **Personal Data Breach**
‘Personal data breach’ means any breach of security leading to the accidental or unlawful destruction, loss, unauthorised alteration, disclosure of, or access to, such personal data.

1.11. **Prior Consultation with the Supervisory Authority**
The Controller shall consult the supervisory authority prior to any processing where such processing would result in a high risk.

2. NATURE OF DATA

In the course of the Company's operations, data is collected in order to enable the provision of its services. This data is necessary for the fulfilment of the Company’s contractual obligations to clients. In addition, the Company works with third party vendors (airline companies, hotels etc.) the data of which is collected as part of this cooperation. The Company also collects personal and sensitive data of its employees, such as sick leaves, pregnancies etc.

Any personal data collected by the Company is ordinary (namely, data relating to the name, e-mail address, ID or passport numbers of clients or persons representing such clients, TIN, profession, address, phone numbers, credit or debit card numbers, and any tax documents necessary to invoice the services provided etc.), The collection and processing of such data is intended to enable the provision of better and faster service by the Company.

3. DATA COLLECTION

Data collection results from entering into contractual relations with clients, vendors and employees. Data is collected by the following departments:

3.1. **Reservations Department**
All data collected by the Reservations Department pertain solely to the operations of the Company and include client data such as the name, phone numbers and e-mail address, ID card or passport details, when this is required (e.g. to issue visas), any taxation details (TIN, tax office, registered office) necessary to issue billing documents, bank account and credit card details needed to settle obligations or claims.

3.2. **Accounting Department**
All data collected by the Accounting Department include client/vendor taxation details, bank account or credit/debit card details and the contact details of the accounting departments of clients or vendors. Such data is collected either by the Reservations Department through direct communication with the clients and/or vendors. The Accounting Department also collects data pertaining to employees of the Company for the purpose of informing tax and social security authorities about the lawful application of all tax and labour laws.

4. DATA PROCESSING

The processing of data collected by the Company is necessary for the performance of its contractual obligations to clients. The data subjects consent to this processing as an act of free choice, knowing the purpose of collecting and processing and their transmission to third parties, for the performance of the services required by the clients. In certain cases, the processing of personal data is necessary for the purposes of our legitimate interests or for the purpose of our compliance with National and/or European legislation.

The Company does not use such data to create profiles to evaluate certain personal aspects relating to the data subjects nor for marketing purposes (newsletters). All data is collected on the basis of the principle of "data minimisation" (as much as necessary) and any special categories of data (of a racial, political, religious, genetic, biometric and sexual orientation nature and other personal data).

The Company shall process any personal data collected and entered in its tax records as well as by electronic means on the computers of the Company and, where appropriate, in case of changes, such data shall be retrieved from such computers, amended and, ultimately, deleted or destroyed.

Furthermore, such data shall be communicated, where appropriate, to the competent authorities (Social Security Institutions, Tax Offices, the Employment Authority and others).

The Controller is the Company itself acting through its Legal Representative, Mrs. Antonia Epifani, resident of Kifissia, with TIN:*****

Such processing may also be performed by any other natural persons (e.g. third party employees or contractors) authorised by the Controller and under his/her direct supervision.

5. TRANSFER OF DATA

As part of our operations, any data collected by the Company may be transferred to third parties or third countries. Such transfer applies exclusively to data required for the provision of services requested by the client and the discharge of other contractual obligations for the implementation of any project. All cooperation agreements between the Company and third parties explicitly stipulate that the contracting third parties must comply with the Regulation. Furthermore, such data may be transmitted to any judicial and/or tax authorities and/or lawyers.

6. RETENTION OF DATA

Personal data is retained for the duration of such relation (contractual obligations) with the data subjects.

The personal data of clients are retained for a period of at least fifteen (15) years to enable the Company to fulfil its obligation to submit accurate information to the tax or other administrative authorities.

7. MANNER OF PROTECTION

7.1. The Company shall keep such personal data in printed and/or electronic form.

7.1.1. The Company shall keep all client, vendor and employee details, as well as any electronic correspondence with the data subjects in electronic form in files stored on an external server installed at its registered office. Each PC has a unique password which is changed from time to time and which is known and managed by Controller and/or any authorised employee working under his/her direct supervision. Any processing by unauthorised users is prohibited. However, in cases where it is absolutely necessary and with the personal responsibility of the Controller or his/her authorised employees, data may be stored on USBs kept under lock and key, as well as on electronic reading devices (PCs and notebooks, tablets and smartphones) owned and used by the Company.

The Company shall update and monitor its security technology on an ongoing basis. The Company shall restrict access to your personal data to employees who need to know such information. In addition, the Company shall provide training to its employees on the importance of confidentiality and non-disclosure as well as on the security of personal data. Among other means, the Company applies technical and administrative measures and procedures to protect such data from any loss, alteration, unauthorised processing or modification, including but not limited to

encryption, detection and management of security breaches, *use of information systems and software installed on PCs in such a way that minimises the use of personal data and/or user identification data*, adoption of individual procedures for the retention and safe deletion/destruction of personal data.

Copies of all data kept in electronic form are also kept in back-up files stored on an external hard disk kept in the Director's office that can be locked, and the only person who has the key is the Legal Representative of the Company. All electronic devices where personal data is stored must not be exposed in places accessible to the public or where their display screen can be viewed by any person other than the authorised users of such devices.

7.1.2. The Company keeps paper-based files of clients, vendors and employees (and, specifically, documents including the details of clients, vendors, employees and others) that are stored in cabinets or archive boxes secured with locks in the Company's administration offices which are accessible only by the Legal Representative/Controller of the Company, and the Company has also installed an alarm and fire warning system.

8. DATA SUBJECTS RIGHTS

8.1. Should any data subject request information on any data retained by the Company about them that is subject to processing, the Company shall provide the data subject, in writing or by other means, including by electronic means, any information requested, in a concise, transparent, intelligible and easily accessible form, using clear and plain language

This information, which is provided free of charge, is given without delay and, in any case, within one month from receipt of such request, a time limit that may be extended by one more month by written notification of the data subject.

8.2. The Company shall inform the data subject accordingly with a notice which includes the identity and contact details of the Controller or his authorised representative, the legal interest of the Controller justifying such processing, the categories of personal data subject to processing, the recipients or categories of recipients of personal data, the notice of transfer of data to third parties, the period of retention of data files, the right of data subjects to access, edit and limit the processing of their data, as well as the right to object to such processing, the right to lodge a complaint with a supervisory authority and the right to withdraw at any time his/her consent for data processing of the data subject that provided such consent.

8.3. Should any data subject submit a request to cease the collection of data/permanently delete such data or a request to use the right to be forgotten, the Company shall take immediate action, with the due diligence of the Controller and Legal Representative of the Company, to cease the collection of such personal data and the permanent deletion of any data already collected, by delivering such data to the data subjects, with acknowledgment of receipt, or through the permanent destruction (by shredding or other means) or permanent deletion of such data from the Company's PCs.

This 1st version of the Code is subject to revisions.

Maroussi, 24/05/2018
On behalf of T&T EXECUTIVE SA

The Controller