GuestTek

Connect Confidently

Privacy and Data Protection Policy

I. INTRODUCTION

This Privacy and Data Protection Policy ("Policy") outlines the standards that the companies within the GuestTek organization ("**GuestTek**") adhere to when Processing Personal Data of various stakeholders, which are defined below. This Policy does not replace any specific data protection requirements that might apply to a corporate function or business unit.

This Policy is realized through related Policies and Standard Operating Procedures (SOPs). Policies and SOPs are developed in a manner that will ensure that GuestTek conducts its business in compliance with the respective national and international data protection and confidentiality laws, regulations and guidelines and Processing of Personal Data and respects the needs of GuestTek Stakeholders for protection of their Personal Data.

Such regulations, laws and guidelines include, but are not limited to EU Directives 95/46/EC, and 2002/58/EC on Data Protection and the Regulation (EU) 2016/679 (hereinafter referred to as the "GDPR") and resultant national Privacy and Data Protection Acts within the EU and US and other national laws and standards, as apply from country to country ("**Applicable Laws**"). As of the effective date of this Policy, the European regulations governing transfer of confidential information outside of the EEA are changing, but GuestTek will adhere to the most current version of all Applicable Laws and will revise this Policy as necessitated by revisions to those laws.

GuestTek in the United States adheres to the Privacy Shield Principles concerning the transfer of Personal Data from the EU and Switzerland to the United States of America. Accordingly, GuestTek follows the Privacy Shield Principles and Frequently Asked Questions, published by the U.S. Department of Commerce, with respect to all such Personal Data. For additional information about the Privacy Shield Program please visit: https://www.privacyshield.gov.

Compliance with this Policy

It is important that GuestTek complies fully with Applicable Laws, as a failure to comply with such laws may amount to a criminal offence by GuestTek and its Employees. In order to achieve compliance with Applicable Laws, it is essential that all Employees follow this Policy.

Each new Employee to GuestTek, as part of their induction/orientation to the company is:

- Required to sign a non-disclosure agreement provided by Human Resources; and
- Provided with access to this Policy and made aware of any privacy and confidentiality requirements as is pertinent to their role. This is irrespective of the contract type e.g., permanent, temporary, and evidence of this will be stored in each individual's Personal Training Record.

GuestTek's processes with respect to privacy and data protection may be audited (internal or external audit) or undergo inspection by Regulatory Authorities. This may include investigation into how individuals implement these processes as part of their role. Project Managers and Line Managers are responsible for retaining an oversight of the maintenance of privacy and confidentiality by Employees on their studies and within their departments during conduct of their routine activities.

Non-compliance with this Policy will result in disciplinary action, which may include termination of employment, and/or action for breach of contract. This Policy does not form part of Employee contracts of employment and it may be amended at any time.

Note: Protection of confidential business information of clients and vendors is addressed in the Information Security Policy, and the steps taken in relation to the Processing of Employee (defined below) Personal Data is dealt with in the Global Employee Privacy and Data Protection Policy.

II. DEFINITIONS

"**Stakeholder Data**" or "**Data**" means any Personal Data relating to a Stakeholder.

"**Stakeholder(s)**" means all contacts of GuestTek (save for Employees), including the following:

- clients;
- vendors;
- shareholders;
- other business partners.

"**Employees**" means all current and past GuestTek employees (including employees of wholly owned subsidiaries, working under permanent or fixed-term employment contracts), including trainees, temporary staff, contractors and consultants who are given access to GuestTek's IT systems. Specific processing of employee's Personal Data is addressed in Global Employee Privacy and Data Protection Policy.

"**Personal Data**" means any information, which alone or when combined with other information, relates to an identified or identifiable living individual. An identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to that person's physical, physiological, mental, economic, cultural or social identity. Examples of data that may permit this kind of identification in the Stakeholder data processing context include but are not limited to identification data (such as name), professional contact details (such as telephone number, email, address) and professional status (such as title, position, location).

"**Processing**", "**Process**" or "**Processed**" means any operation or set of operations performed upon Stakeholder Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer, remote access or otherwise making available, alignment or combination, blocking, erasure or deletion.

"Pseudonymized Data" means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. There is a greater risk of individuals being identified than with anonymized data.

"**Sensitive Personal Data**" is a subset of Personal Data that contains information relating to a person's race or ethnic origin; political or philosophical opinions; religious beliefs; physical or mental health or condition; sexual history, preference or orientation; genetic data; biometric data; trade union membership or affiliation; and criminal history.

1. DATA PRIVACY PRINCIPLES

The data privacy principles below are the foundation of this Policy. As such, GuestTek will, through appropriate management and controls on an on-going basis, monitor implementation of and compliance with these principles.

1.1 Lawfulness, fairness and transparency

It is a fundamental principle within GuestTek that any Stakeholder Data is processed fairly, sensitively, respectfully and in accordance with this Policy and Applicable Laws.

GuestTek will provide Stakeholders with an adequate Privacy Notice at the point of data collection, in order to inform Stakeholders about the purposes for which it collects their Personal Data, how to contact the relevant GuestTek entity if they have any queries or complaints about the processing of their Personal Data, and the administrative process by which the complaints will be resolved. Where appropriate, GuestTek will communicate the types of third parties to which GuestTek discloses Stakeholder Data, and the choices, procedures and means GuestTek offers for limiting use and disclosure of Personal Data.

1.2 Purpose Limitation

GuestTek will ensure that all Stakeholder Data is collected for specified, explicit and legitimate purposes and is not processed in a way incompatible with those purposes.

1.3 Data minimisation

GuestTek will collect and process Stakeholder Data only to the extent that such Data is adequate, relevant and limited to what is necessary to fulfil legitimate business purposes, and/or to comply with legal requirements, including those legal requirements of the countries in which the Stakeholder Data was collected, as applicable.

1.4 Data Accuracy

GuestTek will take every reasonable step to ensure that all Stakeholder Data is accurate, complete, current, and where necessary, is kept up to date. Where the Data are inaccurate having regard to the purposes for which they are processed, GuestTek shall erase or rectify such Data without delay. All Stakeholders have a responsibility to assist GuestTek in this effort (e.g., by notifying their local contact at GuestTek in a timely manner when their Personal Data has changed).

1.5 Data Retention

GuestTek will not keep Stakeholder Data for longer than is necessary to fulfil the purpose(s) for which it was collected. In certain cases, Stakeholder Data may be kept for an extended period of time in order to comply with legal obligations, or for the establishment, exercise or defence of a legal claim, or to comply with GuestTek's policies, in accordance with applicable law.

1.6 Data Security

All Data collected by GuestTek will be processed in a way that ensures appropriate security of such Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisation measures as needed.

1.7 Sensitive Personal Data

Data protection legislation imposes additional safeguards for Sensitive Personal Data, for example, tighter obligations around when such data can be collected and the need for explicit consent when collecting and using Sensitive Personal Data. While GuestTek aims at minimising the amount of Sensitive Personal Data that it processes in relation to Stakeholders, GuestTek may nonetheless process such Data where there is an appropriate legal basis for processing.

1.8 Marketing

Where required under Applicable Laws, GuestTek will offer Stakeholders the opportunity to choose (opt-in) whether they receive communications from GuestTek or our affiliates in relation to GuestTek products and services. Stakeholders may opt-out of receiving marketing materials at any time by emailing GDPRinfo@guest-tek.com to remove consent.

2. TYPES OF PERSONAL DATA COLLECTED

2.1 Data collected as part of general business activities

GuestTek may collect Stakeholder Data as part of its general business activities. Such Data may include, but is not limited to:

- identification data, such as first and last name;
- contact details (including professional and personal, as appropriate), such as address, telephone number and email address;
- employment details, such as job title and office location;
- financial data, such as bank account details, in order to fulfil contractual obligations and related purposes;
- information relating to the Stakeholder's transaction with us and fulfilment of their order;
- information that Stakeholders provide in correspondence with us, for example, when making any enquiry or complaint, completing a survey, reporting a problem with a GuestTek system, providing feedback to us and other business activities.

2.2 Data collected by automated means

GuestTek may also collect certain information by automated means (e.g., log-files, IP address, navigation history and other communication data) whenever a Stakeholder logs on to GuestTek's information systems network and/or uses its IT resources, whether for our own billing purposes or otherwise. Subject to legal restrictions, this information may be used to monitor GuestTek's IT resources and for the maintenance and security of GuestTek's information systems network.

2.3 Purposes of the Processing

The purposes for which GuestTek collects Stakeholder Data may include, but is not limited to:

- as part of its provision of products and services to its Stakeholders;
- to carry out our obligations arising from any contracts entered into with Stakeholders;
- to carry out obligations arising from regulations and legislation;
- to provide Stakeholders with information, products or services that they request from us or which we feel may interest them, where they have consented to be contacted for such purposes;
- in order to improve our service to Stakeholders with respect to GuestTek products and services that are available from time to time;
- to notify Stakeholders about changes to our service, updates to our website, new GuestTek product offerings or special events hosted by GuestTek or our business partners;
- to send Stakeholders marketing materials (where in accordance under Applicable laws) relating to GuestTek's products or services;
- to protect the rights, property, or safety of GuestTek, our Employees, or others.

3. TRANSFER AND SHARING OF INFORMATION

GuestTek takes precautions to allow access to Stakeholder Data only to those Employees who require such access to perform their job duties and to third parties who have a legitimate purpose for access to such Data. Stakeholder Data may be transferred to GuestTek sites in countries other than the country where the Data was captured. The same high level of security and protection of personal information is applied in all geographies through appropriate procedures and contracts.

3.1 Group entities

Stakeholder Data may be shared among GuestTek's group of companies for purposes consistent with this Policy.

3.2 Vendors, suppliers and other service providers

GuestTek may share or disclose Stakeholder Data with vendors, suppliers and other service providers who have been selected by GuestTek to perform specific activities on behalf of GuestTek (such as IT hosting providers or corporate card companies). GuestTek will only select vendors, suppliers or other service providers who have demonstrated by satisfactory completion of an assessment that they can comply with GuestTek's and other applicable legal standards. Any service providers engaged by GuestTek will have access to Stakeholder Data solely to the extent necessary to enable them to perform those services on GuestTek's behalf and GuestTek will ensure that they are contractually prohibited from using Stakeholder Data for any other purpose.

All service providers must enter into a services agreement or Confidentiality and non-Disclosure Agreement ("CDA") with GuestTek whereby they are required to appropriately safeguard the privacy and security of Stakeholder Data they process on behalf of GuestTek. Where GuestTek has knowledge that a service provider is using or disclosing Stakeholder Data in a manner contrary to this Policy, GuestTek will take reasonable steps to prevent or stop the use or disclosure of Stakeholder Data to that service provider.

3.3 Other third parties

GuestTek may also share or disclose Stakeholder Data with other third parties, such as regulatory authorities, sponsors, or where otherwise required by applicable local laws (such as government agencies or ministries).

It is occasionally necessary that GuestTek must provide access to its Policies, SOPs, Working Guidelines and other business critical information to third party contractors, regulatory authorities and other business partners. Where there is no contractual provision to assure confidentiality of GuestTek's materials, a CDA will be sought to permit release of such materials. A CDA may not be necessary in the instance of an audit by a regulatory authority, which is bound to protect sensitive information by its governing laws and regulations.

GuestTek may disclose Stakeholder Data to third parties without the data subject's knowledge or consent where it is: (i) necessary to comply with the law or to protect the safety of GuestTek Employees; (ii) to respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims; (iii) to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, or (iv) as otherwise required by law.

4. INFORMATION SECURITY

4.1 General security measures

Stakeholder Data is only as secure as the security mechanisms employed on the system(s) on which the data is maintained. GuestTek up holds a high level of security to protect all Stakeholder Data and employs industry standard security measures designed to protect against unauthorized access, loss, misuse or alteration of Stakeholder Data.

Computer systems, equipment, networks, programs, data, and documentation are secured to the extent reasonably possible using existing technology, and as regulated by the drug and device research regulatory authorities. Appropriate physical and logical security systems are in place, to protect paper and electronic records/documents from unauthorized access, damage or loss, for example:

4.1.1 Internet based

GuestTek uses externally facing mechanisms such as secure web portals and file transfer (SFTP) sites for secure information exchange with sponsors. The Information Security Policy covers the measures employed to assure the privacy and confidentiality of information captured and made available via these mechanisms.

4.1.2 Database

The Information Security Policy and its associated SOPs collectively cover the measures employed to assure the privacy and confidentiality of information captured and processed in GuestTek's databases.

4.1.3 Email

All GuestTek Employees are individually responsible for all electronic mail sent from their account and for the appropriate handling of Personal Data received into their account. Care should always be taken to evaluate whether e-mail is the most appropriate method for dissemination of Personal Data.

4.1.4 Telephone

Where communication of information is by telephone, care will always be taken to evaluate whether this is the most appropriate method for dissemination of sensitive information.

4.1.5 Paper based Information

Paper based information that is current and required for on-going study and other activities must be maintained, wherever possible, in locked cupboards or otherwise restricted areas. When information ceases to be required, it is destroyed confidentially, by shredding.

Access to information and systems is restricted to appropriate Employees. For further information on the measures employed to assure the security of Stakeholder Data captured and processed on the GuestTek corporate network please refer to the Information Security Policy and its associated SOPs.

Note that although GuestTek takes steps to ensure the integrity of GuestTek Stakeholder Data, it is the responsibility of each Employee to ensure that GuestTek Stakeholder Data is kept as accurate, complete and current as possible by informing GuestTek of any changes or errors.

4.2 Security measures for transit of Data

Where electronic Stakeholder Data is to be transferred on physical media, the media will be appropriately password protected or encrypted to minimize the risk of unauthorized access to that information. Additionally, passwords used to secure electronic information will be passed to the recipient using a separate means of communication to prevent compromise (i.e. if a CD is being mailed, the password may be transmitted telephonically or emailed or if data is being emailed, the password(s) must be transmitted via separate email, telephone or postal mail).

For Employees who travel as part of their role, baggage containing electronic hardware or information on other media e.g., paper will not be left unattended, or in the custody of anyone unauthorized to be in possession of that information. If air travel is necessary, laptops and sensitive information should, where security permits, be carried as hand luggage.

Where it is necessary to transfer Personal Data (paper based or electronic data on physical media) to other locations (e.g., to other GuestTek offices or external archive facilities), the information will be securely packaged. Tamper evident tape, if available, or other suitable sealing materials (e.g., security tags) will be used to seal the container or box to provide a measure of assurance of the integrity of the materials during transfer. The transfer of documents or other media will be tracked appropriately.

4.3 Security measures in place with third parties.

4.3.1 Vendors

For all instances in which GuestTek engages the services of a vendor (for example for Support Services or On-site resources), the responsibilities of both GuestTek and the vendor will be clearly established by means of contract and/or CDAs as appropriate. These documents must be executed prior to initiation of any business and before any transfer of Personal Data takes place.

All vendor audits, conducted prior to or during an engagement to provide services will include examination of the vendor’s processes for handling Personal Data to ensure compliance.

5. RETENTION AND ARCHIVING OF INFORMATION

GuestTek retains Stakeholder Data for as long as required to carry out the purposes described in this Policy or as otherwise needed to comply with Applicable Laws. Once GuestTek no longer needs a Stakeholder's Personal Data, it shall either delete the Data or archive it and restrict its further access or use, in line with the GuestTek Data Retention Policy and the relevant SOPs.

6. DATA TRANSFERS

As a global organisation GuestTek needs to transfer Stakeholder Data to countries around the world. In particular, such transfers are necessary to facilitate the global management and administration of GuestTek's Stakeholder transactions, as well as for the global security and maintenance of GuestTek's IT systems and network.

GuestTek will carry out regular transfers of Stakeholder Data from countries within the European Economic Area (EEA) to countries outside of the EEA, such as the United States of America. Countries within the EEA maintain a certain level of protection for Personal Data that may not be present in countries outside of the EEA and as such certain safeguards need to be in place to protect the information.

Where a GuestTek entity must transfer Stakeholder Data outside the EEA, it shall do so on the grounds of either: i) an adequacy decision that has been pronounced by the European Commission recognising the adequate level of protection for Personal Data of the third country, or territory, or sector within that third country, or of an international organisation; or ii) appropriate safeguards that were implemented by GuestTek to protect the Data that are being transferred. Such appropriate safeguards may rely, for example, on the existence of Standard Contractual Clauses that are entered into between the exporting and the importing entities, or on the Privacy Shield of both GuestTek and the recipient.

When transferring Stakeholder Data globally, GuestTek ensures that only authorized personnel who require access to the Data to perform their job duties shall be given access to such Data on a need-to-know basis.

6.1 Privacy Shield

GuestTek and its affiliated companies in the United States adhere to the EU-US Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from the European Union member countries and Switzerland to the United States. GuestTek adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability as published by the U.S. Department of Commerce.

In response to the European Court of Justice's decision in October 2015 to invalidate the Safe Harbor agreement between the European Commission and the U.S. Department of Commerce, GuestTek has undertaken a review of the mechanisms and processes by which all transfers and processing of personal data are handled. GuestTek is committed to maintaining the highest feasible level of protection and continues to abide by all Applicable Laws which govern these processes, including registration with Privacy Shield. GuestTek will implement additional measures to ensure the confidentiality, integrity and availability of personal information we process if the laws change again, and will put in place other mechanisms to ensure a compliant transfer of personal information from European Union member countries to the U.S.

7. DATA SUBJECTS' RIGHTS.

Stakeholders have a right to access and obtain a copy of their Personal Data, and to request that their Personal Data be rectified where it is inaccurate. Stakeholders may further request that their data be erased or restricted where the Data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, in accordance with applicable laws. Stakeholders may also object to the processing of their Personal Data where GuestTek:

- makes decisions in relation to the Stakeholder based solely on automated processing, including profiling;
- Processes such data for marketing purposes; and/or
- where GuestTek has a legitimate interest for collecting and processing such data, unless GuestTek demonstrates compelling legitimate grounds to continue processing such data, or where such processing is necessary for the establishment, exercise or defence of legal claims.

Stakeholders may exercise their rights by contacting the Data Protection Officer by email: GDPRinfo@guest-tek.com. At any time, a Stakeholder may lodge a complaint regarding the processing of their Personal Data by GuestTek with the relevant supervisory authority in the country in which they are established.

8. COMMITMENT AND RESPONSIBILITY

It is the responsibility of all GuestTek Employees to operate within the requirements of this Policy at all times, when processing Stakeholder Data. This is to provide assurance, internally and externally, of GuestTek's commitment to maintaining and respecting the confidentiality of Personal Data and the privacy of any subject of that data.

It is the responsibility of GuestTek to ensure that:

- each Employee signs a Confidentiality Agreement at the beginning of his or her employment;
- new Employees (regardless of status of employment; permanent, contract, etc.) are made aware of this Policy and data protection and security requirements as it pertains to their role upon induction/orientation.

9. COMPLAINTS AND DISPUTE RESOLUTION

Any violations of this Policy must be promptly reported to each Employee's direct supervisor and GuestTek's Data Protection Officer. If the conduct involves a direct supervisor, the next level above the direct supervisor should be advised of the violation or suspected breach, ideally within five (5) business days of discovery.

Complaints or allegations of violations of this Policy should be as detailed as possible, including the names of all individuals involved and any witnesses. GuestTek will directly and thoroughly investigate the facts and circumstances of any asserted violations, and will take prompt corrective action, if appropriate.

No one will be subject to, and GuestTek prohibits, any form of discipline, reprisal, intimidation or retaliation for good faith reporting of violations of this Policy, pursuing any claim that a person's privacy rights have been violated or cooperating in related investigations. GuestTek is committed to enforcing this Policy against all forms of unauthorized disclosure or use of Personal Data.

GuestTek will cooperate with the relevant supervisory authorities in the investigation and resolution of complaints relating to this Policy. GuestTek will seek, as soon as possible, to comply in good faith with the advice of these authorities.

10. COMPLIANCE WITH LAWS

Processing of Stakeholder Data will be conducted in accordance with Applicable Laws.

11. WHO TO CONTACT

For any questions or comments in relation to this Policy, or GuestTek's privacy practices, or to request access to Personal Data, please send an email to the Data Protection Officer at: GDPRinfo@guest-tek.com

12. POLICY REVISION HISTORY

Version	Description of changes	Effective date
1.0	Contact details GDPRinfo@guest-tek.com	25th May 2018
2.0	Word Clinical – removed	07th June 2018

13. AUTHORISATION

Author: *(Official Signature on File).*

Date