

DATA SECURITY POLICY

FORTY FIVE POSITIVE TECH PRIVATE LIMITED (hereinafter the “Company / We / Data Processor”), operating under the brand name SPALBA, is committed to complying with Data Security Legislation of all geographical territories we cater to, in order to protect the personal privacy of all legal and natural individuals including but not limited to our customers and third parties whose data we hold. This policy outlines how the Company will comply with Data Security obligations when handling personal data relating to our customers and other third parties.

We handle the personal data of our customers and other third parties (hereinafter the “Third Party”) as data processors. We understand we have we have specific legal obligations to protect that data in our possession for processing. We ensure that all personal data relating to its customers and other third parties is handled securely and with proper regard for their privacy. Compliance with this policy will help ensure that all personal data held by us is handled lawfully.

All employees and associates of the Company are required to comply with this Policy. Any deliberate breach of this policy will result in disciplinary action, which may include dismissal and possible prosecution.

1. DEFINITIONS

- i. **“We”, “Our”, and “Us”** shall mean and refer to the Company, as the context so requires.
- ii. **“Third Party”** means an actual or prospective customer, distributor, reseller, vendor, supplier, consultant, professional adviser, business partner or any other third party that does or may do business with the Company.
- ii. **“Personal Information”** shall mean and refer to any personally identifiable information that we may collect from you such as Name, Email Id, Mobile number, Password, etc. For removal of any doubts, please refer to Clause 2 of the Privacy Policy.

2. PERSONAL DATA PROCESSED, AND CATEGORIES OF DATA SUBJECTS

- i. Categories of personal data

The categories of personal data processed are:

- personally, identifiable information (e.g. name, surname, email)
 - statistical or other usage data observed on the internet (e.g. via analytics, services etc.)
 - customer history
 - billing, invoicing and payment data
 - other: Third party data collected during events and conferences or MICE
- ii. The personal data collected will be processed for enabling the functionality of the software and applications as authorized in accordance with GDPR and CCPA

3. DATA SECURITY PRINCIPLES

The data protection principles listed below are the foundation of this Policy:

i. Lawfulness, fairness and transparency

The Company shall process Personal Information fairly, and in compliance with this Policy and applicable laws.

ii. Data Accuracy

The Company will take all reasonable steps to ensure that Personal Information is accurate and complete and will rectify or erase any incorrect Personal Information without delay.

iii. Purpose Limitation

The Company will ensure that Personal Information collected is for specified, explicit and legitimate purposes and only to the extent necessary to fulfil those purposes.

iv. Data Retention

The Company will only keep Personal Information only till it is necessary to fulfil the purpose(s) for which it was collected or to comply with territorial legal restrictions of the Third Party.

v. Data Security

All Personal Information collected will be processed in a secure manner by the Company.

4. OBLIGATIONS OF THE COMPANY

The Company warrants and undertakes that:

- i. It will comply with all applicable law including Applicable Data Protection law in the execution of the policy.
- ii. It will not appoint sub-processors to process the Personal Data on its behalf without the prior written approval of the Data Controller.
- iii. It will have in place appropriate technical and organisational measures, and all measures pursuant to Article 32 of the GDPR and all other Data Protection legislations as set out in Clause 8 of the present Policy, to protect the confidentiality of the Personal Data and to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.
- iv. It will obtain guarantees from any sub-processors processing the Personal Data, that they will have in place appropriate technical and organisational measures, and all measures pursuant to Article 32 of the GDPR, to protect the confidentiality of the Personal Data and to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.
- v. It will have in place procedures so that any individual party it authorises to have access to the Personal Data, including employees of the Company, will respect and maintain the confidentiality and security of the Personal Data. Any person acting under the authority of the Data Processor shall be obligated to process the Personal Data only on instructions from the Company. This provision does not apply to persons authorised or required by law or regulation to have access to the Personal Data.
- vi. It will not disclose any Personal Data to any external sources in any circumstances unless such disclosure is necessary in order to fulfil the purpose for which it has been collected, or is required by applicable law.
- vii. It will give the Third-Party prompt notice of a Personal Data breach or a potential data breach, once becoming aware of same, and the Company will cooperate with the Third Party in implementing any appropriate action concerning the breach or the potential breach as the case may be, including corrective actions.

- viii. It will delete from its systems all soft copies of any Personal Data and return all soft and hard copy documentation on the completion of the purpose for which it has been collected or on request from the Third Party and will do so in a timely manner, giving a written confirmation of same having been done.
- ix. Without prejudice to other legal provisions concerning the Third Party's right to compensation and the liability of the parties generally, as well as legal provisions concerning fines and penalties, the Company will carry full liability in the instance where it or its sub-processor is found to have infringed applicable law including Applicable Data Protection law through his processing of the Personal Data.
- x. It will be capable of demonstrating its compliance with the obligations of Applicable Data Protection law.

5. THE COMPANY'S USE OF THIRD-PARTY INFORMATION

The information provided by you shall be used to provide and improve the service for you and all users.

- a. For maintaining an internal record.
- b. For enhancing the Services provided.

Further, the third party's personal data may be collected and stored by us for internal record.

We use the third party's tracking information such as IP addresses, and or Device ID to help identify you and to gather broad demographic information and make further services available to you.

We will not sell, license or trade the third party's personal information. We will not share the third party's personal information with others unless they are acting under our instructions or we are required to do so by law.

Information collected via our server logs includes users' IP addresses and the pages visited; this will be used to manage the web system and troubleshoot problems. We also use third-party analytics, tracking, optimization and targeting tools to understand how users engage with our Platform so that we can improve it and cater personalized content/ads according to their preferences.

6. HOW INFORMATION IS COLLECTED

Before or at the time of collecting personal information, the Company will identify the purposes for which information is being collected. If the same is not identified to the Third

Party, they have the right to request the Company to elucidate the purpose of collection of said personal information, pending the fulfilment of which you shall not be mandated to disclose any information whatsoever.

The Company will collect and use the third Party's personal information solely with the objective of fulfilling those purposes specified by the Company in Clause 1 of the Policy, within the scope of the consent of the individual concerned or as required by law. The Company will only retain personal information as long as necessary for the fulfilment of those purposes. We will collect personal information by lawful and fair means and with the knowledge and consent of the individual concerned.

Personal data should be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, should be accurate, complete, and up-to-date.

7. SENSITIVE PERSONAL DATA

The Company does not normally hold sensitive personal data relating to customers or other third parties. However, personal data falling within these categories is subject to additional protection and, therefore, where sensitive data is collected for any reason, we endeavour to obtain consent from the owner of such data.

8. DISCLOSURE OF INFORMATION

Information collected will not be considered as sensitive if it is freely available and accessible in the public domain or is furnished under any of the legislations governing the present policy.

Due to the existing regulatory environment, the Company cannot ensure that all of your private communications and other personally identifiable information will never be disclosed in ways not otherwise described in this Policy. By way of example (without limiting and foregoing), the Company may be forced to disclose information to the government, law enforcement agency or any external parties. Therefore, although the Company standard practices to protect your privacy, the Company does not promise, and you should not expect, that your personally identifiable information or private communications would always remain private. We do however assure you that any and all disclosure of your personally identifiable information shall be personally intimated to you through an email sent to your provided email address.

As a matter of policy, we do not sell or rent any personally identifiable information about you to any third party. However, the following describes some of the ways that

your personally identifiable information may be disclosed:

- a. **External Service Providers:** There may be a number of services offered by external service providers that help you use our Platform. If you choose to use these optional services, and in the course of doing so, disclose information to the external service providers, and/or grant them permission to collect information about you, then their use of your information is governed by their privacy policy.
- b. **Law and Order:** We cooperate with law enforcement inquiries, as well as other third parties to enforce laws, such as intellectual property rights, fraud and other rights. We can (and you authorize us to) disclose any information about you to law enforcement and other government officials as we, in our sole discretion, believe necessary or appropriate, in connection with an investigation of fraud, intellectual property infringements, or other activity that is illegal or may expose us or you to legal liability.

9. RIGHTS OF THE THIRD PARTY

Unless subject to an exemption, The Third Party owning the data have the following rights with respect to their personal data:

- b. The right to request a copy of your personal data which we hold about you;
- c. The right to request for any correction to any personal data if it is found to be inaccurate or out of date;
- d. The right to withdraw Your consent to the processing at any time;
- e. The right to object to the processing of personal data;
- f. The right to lodge a complaint with a supervisory authority.
- g. The right to obtain information as to whether personal data are transferred to a third country or to an international organization.

Where you hold an account with any of our services, you are entitled to a copy of all personal data which we hold in relation to you. You are also entitled to request that we restrict how we use your data in your account when you log in.

10. DELETION AND RETURN OF PERSONAL DATA

- i. The Company shall not create copies or duplicates of the data without the Third Party's knowledge and consent, except for backup copies, insofar as they are necessary for ensuring that data is processed correctly, and where the retention of such data is required by law.
- ii. After conclusion of the provision of services as set out in Service Agreement, the Processor shall, at the discretion of the Third Party who owns the data, either delete in a data-protection compliant manner or return to such Third Party, all the personal data collected and processed under the present Agreement, unless any applicable legal provision requires further storage of the personal data.
- iii. In any case, the Company may retain beyond termination of the contract all the information necessary to demonstrate the compliance of the processing activities carried out.
- iv. The information referred to under sub clause (iii) of the present clause, shall be stored by the Company in accordance with the applicable retention periods, statutory or otherwise determined. The Company may hand the documentation over to the Third Party upon termination of the agreement. In such case, the Company is relieved from any obligation to keep such information or any documentation of the same.

11. SECURITY

The Company will treat your data as an asset that must be protected against loss and unauthorized access. We employ many different security techniques to protect such data from unauthorized access by members inside and outside the Company.

The Company is committed to ensuring that all staff with data handling responsibilities receives appropriate training in relation to data security and confidentiality. In addition, our policy detailing Employee Data Protection Obligations can be found here: The Company recognises that the use of external contractors to handle personal data usually creates additional data security risks. The Company acknowledges that a specific requirement of Data Protection Legislation, is that any contractors that are engaged to handle personal data behalf of the Company, must be carefully selected and properly supervised. Therefore, whenever a contractor is engaged to carry out work that involves the processing of personal data, the Company will allow such contactor to handle personal data only if we are satisfied that the contractor's data security measures are adequate and only where a written contract setting out the contractor's obligations in relation to that data are clearly set out in

accordance with Data Protection Legislation.

However, as effective as encryption technology is, no security system is impenetrable. Our Company cannot guarantee the security of our database, nor can we guarantee that information you provide won't be intercepted while being transmitted to the Company over the Internet.

12. DATA SECURITY BREACHES

Any data security breach should be reported to the Company through mail to irt@spalba.com so that action can be taken to protect affected individuals and to ensure that the risk of recurrence is minimised. If the Company discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of the third party, it will report it to the appropriate legal authority within 72 hours of discovery. The Company will record all data breaches regardless of their effect. If the breach is likely to result in a high risk to the rights and freedoms of the owner of the data, it will inform the affected person of the breach and provide them with information about its likely consequences and the mitigation measures the Company has taken.

13. SEVERABILITY

Each paragraph of this Policy shall be and remain separate from and independent of and severable from all and any other paragraphs herein except where otherwise expressly indicated or indicated by the context of the agreement. The decision or declaration that one or more of the paragraphs are null and void shall have no effect on the remaining paragraphs of this privacy policy.

14. AMENDMENT

The Policy may change from time to time. The most current version of the policy will govern our use of your information and will always be at the Platform. Any amendments to this Policy shall be deemed as accepted by the User on their continued use of the Platform.

15. CONSENT WITHDRAWAL, DATA DOWNLOAD & DATA REMOVAL REQUESTS

To withdraw your consent, or to request the download or delete your data with us for any or all our products & services at any time, please email to irt@spalba.com

16. CONTACT US

If you have any questions or concerns regarding this privacy policy, you should contact us by sending an e-mail to info@spalba.com