FORT KNOX RESOURCING AND OUTSOURCING
Privacy Policy

This privacy policy applies to all personal data collected by Fort Knox Resourcing and Outsourcing Limited (hereinafter "FKRO") via the internet. FKRO recognizes the importance of your privacy, and that you have a right to control how your personal data is collected and used. We know that providing personal information is an act of trust and we take that seriously. Unless you directly give us consent to do otherwise, FKRO will only collect and use your personal data as set out below.

1. Scope and Applicability

The scope of this Privacy Policy applies to FKRO and any of our affiliates with whom we may share Personal Data, and encompasses all of our Services (operated offline, online, or both) including services made available through the FKRO website (collectively referred to as the "Services") and when you otherwise interact with us, such as through our customer service channels.

2. Data Controller and Data Protection Officer

FKRO may act as a data processor or a data controller depending on the Service being provided and the amount of control we have over the purpose(s) and means of the data processing. We have appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to this privacy policy. If you have any questions about this privacy policy, including any requests to exercise your legal rights, please contact the DPO using the details set out below:

a. Email address: _____
b. Telephone Number: _____

ii. Please note that any Personal Data provided to the Us by Our clients or any other third party is collected by the clients and third parties under their respective privacy and data protection policies. This Policy does not govern any other information or communications that may have been collected by such parties.

iii. You agree that FKRO reserves the right to take any legal or other action against You including the right to deny the usage rights to the website and the Services and referral to the appropriate authorities.

iv. For the purpose of this Policy, the term "Personal Data" refers to any information relating to an identified or identifiable individual and includes the information that

relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

3. Changes to The Privacy Policy

We keep our privacy policy under regular review. This version was last updated on 01/12/2024. We may amend this privacy policy at any time by publishing a revised version of our Product. The revised version shall **become effective 7 days after publication.**

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

4. How we collect and process information about you:

i. From your employer in connection with your job and how it relates to us.
ii. If you use any website operated by us.
iii. From third parties we work closely with (including, for example, business partners, sub-contractors in technical, payment and delivery services, advertising networks, analytics providers, and search information providers). We will notify you when we receive information about you from them and the purposes for which we intend to use that information.
iv. If you access the website or use the Services through a third-party connection or log-in, you authorize Workforce to collect, store, and use, in accordance with this Policy, any and all information available to Workforce through the third-party interface.

5. The Information we collect about You

We collect and use Your Personal Data depending on the Services and the manner You interact with Us. The following categories of Personal Data is collected by Us to provide better services and offerings to You.

i. *Contact Information:* This category includes data such as your name, company name, email address, postal address, telephone number and other contact details that you provide by completing forms on the website or using the Service, including information about you if you register as a user of the website or subscribe to a Service, information about you that you upload or submit to the website or Service, or information you provide to us when requesting information or material from us.
ii. *Complaints/Queries:* Information contained in communications you send to us, for example to report a problem or to submit queries, concerns or comments regarding the website (or its content) or the Services.
iii. *Government-issued identification information numbers:* This category includes data such as National Identity Number (NIN), driver's license number, and passport number.

Further, we may collect any Personal Data that would be required by FKRO to ensure compliance with any applicable laws.

iv. *Transaction and Commercial Information:* Information on your company and its operations from any materials you send us*;* information and other details of any transactions made by you through the website including but not limited to name, address, the total number of employees within the organization that will be using the Services and other financial-related information ("Billing Information") provided by you when making transactions through the website or when using our Services.

v. *Inferred Information derived from other information listed in this section:* We create inferred and derived data elements by analysing our relationship and transactional information.

vi. *Online & Technical Information, including internet or other electronic network activity information:* This category includes data such as IP address, MAC address, SSIDs or other device identifiers or persistent identifiers, online user ID, encrypted password, device characteristics (such as browser information), web server logs, application logs, browsing data, viewing data, website and app usage, cookies, web beacons, clear gifs and pixel tags.

vii. *Other Information:* We may collect Your information such as name, age, contact details, preferences, etc. through surveys and forms, when You choose to participate in these surveys etc. When You communicate with or use the Platform to communicate with other users (such as partners) on our platform, We collect information about Your communication and any information You choose to provide.

viii. *Cookies:* When You visit the Platform, We use cookies to automatically collect, store and use technical information about Your system and interaction with Our Platform.

ix. *Permissible information:* To the extent permitted by law, FKRO may record and monitor Your communications with Us to ensure compliance with our legal and regulatory obligations and our internal policies. This may include communications through telephone, by email, via the contact form, via a link contained in an email sent by us or via some other electronic message offered to you, via the chat function, web care, surveys or (panel) surveys, the (mobile) website, if you sign up for newsletters or via social media. This may also include recording of telephone conversations.

x. *Collection of anonymized data:* We may also collect and/or generate anonymized and aggregated information from Your use of the Platform. The anonymized or aggregated information is not Personal Data since We are not able to re-identify You using any means available to Us from that anonymized or aggregated information. The anonymized and aggregated information is used for a variety of functions, including to help Us identify and remediate any bugs, and to improve the performance of Our Platform. We may share this information with third parties

for Our or their purposes in an anonymized or aggregated form that is designed to prevent anyone from identifying You.

xi. *Aggregated data:* We also collect, use and share Aggregated Data such as statistical or demographic data for any purpose. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy policy.

6. Special Categories of Personal Data

Unless provided to Us by Our clients in order to provide a service, we do not collect any special categories of personal data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and/or information about criminal convictions and offences).

7. Failure to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

8. Our Uses of Personal Data

This section contains information on how we use Your data. Information is collected for the purposes stated in this Policy and will not be further processed in a manner that is incompatible with those purposes.

a. To perform the Services requested by you. For example, if you fill out a "Contact Me" web form, we will use the information provided to contact you about your interest in the Services. This data processing is necessary to provide or fulfil a service requested by or for you.

b. To plan and host events. For example, corporate events, host online forums, blogs and social networks in which event attendees may participate, and populate online profiles in relation to the Services. This data processing is necessary to provide or fulfil a service requested by or for you.

c. For financial and payment purposes. For example, for checking financial qualifications and collect payment from you, where applicable. This data processing is necessary to provide or fulfil a service requested by or for you.

d. To communicate with you and send you marketing communications. We may use information to respond to your requests or questions. For example, we might use your personal data, such as your email address, to respond to your customer questions or feedback. (You can object to further marketing at any time by checking and updating your contact details within your account, or/and selecting the "unsubscribe"" link located on the bottom of Workforce's marketing emails.You have the right to contact us at any time to object to the further processing of your information for the purposes of direct marketing to you, including any profiling related to such marketing.)

e. We may use information for security purposes. We may use information to protect our company, a client, and/or our website and apps.

f. Analyze your preferences, interests and behavior in order to provide you with tailored content and the most relevant content and communications;

g. Enforce our Terms and Conditions, enforce our legal rights, comply with applicable law, and respond to government and legal requests.

h. To determine demographics of platform usage.

i. We may use Personal data for promotional purposes. For example, we might provide you with information about new features, updates, new products or special offers from time to time.

j. Business Transfers. For example, we reserve the right to disclose and transfer all of your information, to a successor (or potential successor) company in connection with a merger, acquisition, or sale of all, or components, of our business, or in connection with due diligence associated with any such transaction. Data processing for this purpose is a legitimate business interest.

9. Lawful Basis for Processing.

The Nigerian Data Protection Act 2023 (NDPA) requires that we have a lawful basis for processing your personal data. At least one of the following lawful bases must apply before we process your personal data:

a. **CONSENT:** where you have given consent to the processing of your Personal Data for one or more specific purposes;

b. **CONTRACT:** We collect certain data from you to fulfil the contract we have with you, or to enter into a contract with you. We use this data to:

i. Give you the services we agreed to in line with our Terms and Conditions.
ii. Send you messages about your account and other services you use if you get in touch, or we need to tell you about something.
iii. Exercise our rights under contracts we've entered into with you, like managing, collecting and recovering money you owe us.
iv. Investigate and resolve complaints and other issues.

c. **LEGAL OBLIGATION:** where processing is necessary for compliance with a legal obligation to which we are subject (e.g., for compliance with criminal laws); and

d. **LEGITIMATE INTERESTS:** where the processing is necessary for the purposes of the legitimate interests pursued by us or by a third party, not overridden by your interests or fundamental rights and freedoms (e.g., for product development and analytics purposes).

10. How do we get your consent?

a. Your consent is given when you voluntarily surrender your information to us to facilitate the provision of our services to you.
b. You are also consenting to our processing of your personal data when you log on our website, or subscribe to our email alerts, or when you provide us with your personal data to enable you participate at our events, receive information from us.
c. If we ask for your personal information for a secondary reason, like marketing, we will either ask you directly for your express consent, or provide you with an opportunity to say no.

11. How can you withdraw your consent?

If after providing us with your information, you change your mind, you may withdraw your consent to our continued collection, use or disclosure, or otherwise processing of your information, at any time, by contacting us at _____.

Please note that such withdrawal of consent shall not affect the lawfulness of processing based on consent before withdrawal.

12. How We Share Personal Data

FKRO shares and discloses Personal Data to other parties as needed to provide our Services and operate our business. The categories of other parties (third parties) with whom we may share personal data include:

a. Internally: Your personal data will be used and shared amongst our employees and contractors who are working on providing your services to you on a need-to-know basis.
b. Service Providers—We may share the personal data that you have provided us with certain third-party services, including public and private institutions pursuant to providing a required service, web services providers, developers, security and storage service providers, analytics service providers, and providers used to analyze our websites' and applications' functionalities.
c. Business Services—We may share any category of Personal Data with our business services providers in the operation of our business and facilitation of the Services, including agents, auditors, financial institutions, and professional advisors.
d. Corporate Activities—We may share any category of Personal Data with other companies or entities as part of any reorganization, merger, sale, joint venture, assignment, transfer, or other disposition of all or any portion of our business, assets, or stock. In such case your Personal Data may be transferred to the potential or actual acquirer, successor, or assign.
e. Government and Legal—We may share any category of Personal Data with other parties, including public authorities, as may be required by applicable law, regulation, or legal process.

Note that FKRO will not rent, sell, or share information about you with other people or non-affiliated companies.

13. Data Retention and Disposal

We will only retain personal data on our servers for as long as is reasonably necessary as long as we are providing Services to you. If you have an account with us, Your personal data is kept on our servers after you close your Account to the amount required to meet regulatory requirements and for monitoring, detecting, and preventing fraud. Where we retain your personal data, we do it in accordance with any applicable legal limitation periods.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

Managed accounts: If the Services are made available to you through an organization (e.g., your employer), we retain your information as long as required by the administrator of your account.

Right to deletion: In some circumstances You can ask Us to delete your data: see 'Your Legal Rights' section for further information.

Anonymisation: In some circumstances, we will anonymise your personal data so that it can no longer be associated with you for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

14. Your Legal rights

You have the following rights under the data protection legislations:

a. right to request information from us on how your personal data is processed
b. right of access to your personal data in our custody
c. right to withdraw your consent to us processing your personal data at any time
d. right to object to our processing of your personal data
e. right to request erasure or deletion of your personal data in our custody
f. right to ask that our processing of your personal data is restricted in certain circumstances
g. right to request rectification of your personal data in our custody
h. right to request us to transfer your data to another entity electronically
i. right to lodge a complaint to the regulator—The Nigeria Data Protection Commission.

15. Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

16. The Services are not intended for Children.

Our Services are meant for use by adults only. We do not knowingly collect personally data from children under 13 years.

17. Log Files

FKRO follows a standard procedure of using log files. These files log visitors when they visit our website or app. All hosting companies do this and this is a part of hosting services analytics. The information collected by log files include your Internet Protocol (IP)

addresses, browser type, Internet Service Provider (ISP), date and time stamp, referring/exit pages, and possibly the number of clicks. These are not linked to any information that is personally identifiable. The purpose of the information is for analyzing trends, administering the site, tracking users' movement on the website, and gathering demographic information.

18. Cookies and Web Beacons

Like any other website, FKRO uses 'cookies'. These cookies are used to store information including visitors' preferences, and the pages on the website that the visitor accessed or visited. The information is used to optimize the users' experience by customizing our web page content based on visitors' browser type and/or other information.

You have the right to decide whether to accept or reject cookies on our website. You can also exercise your cookie rights by setting your preferences in the Cookie settings in your browser to disable cookies altogether. Most web browsers can be set to disable the use of Cookies. You can usually find these settings in the "options" or "preferences" menu of your browser.

However, if you disable Cookies on our website, you may not be able to access functionality on our Website correctly or at all.

You may also clear cookies from your computer via your web browser settings. You may also wish to use a Google Analytics opt-out web browser add-on. Information on this option is available at:
http://support.google.com/analytics/bin/answer.py?hl=en&answer=2700409

19. Third-Party Sites, Blogs, and Social Media

Our website may include links to other websites whose privacy practices may differ from ours. When you use a link to go from our website to an unaffiliated website, the privacy policy of the other website will apply.

20. Transfers of Personal Data.

We may need to transfer your Personal Data outside of the country from which it was originally provided. This may be FKRO or third parties that we work with who may be located in jurisdictions outside Nigeria, the EEA, Switzerland and the UK which have no data protection laws or laws that are less strict compared with those in Europe. Whenever we transfer Personal Data outside of the EEA, Switzerland or the UK, we take legally required steps to make sure that appropriate safeguards are in place to protect your Personal Data. Such transfers will be made pursuant to the standard data protection clauses adopted/approved by the Nigerian Data Protection Commission. In the event that the

Commission or courts determine that the transfer mechanism above is no longer an appropriate basis for transfers, FKRO and customer shall promptly take all steps reasonably necessary to demonstrate adequate protection for the Personal Data, using another approved mechanism.

21. Data Security Strategies

We have appropriate physical, electronic, and managerial procedures to safeguard and help prevent unauthorized access and maintain data security of, and to use correctly, the information we collect online. These safeguards vary based on the sensitivity of the information that we collect and store. All information you provide to us is stored on our secure servers. Where we have given you (or where you have chosen) a password which enables you to access certain parts of our Site, you are responsible for keeping this password confidential. We follow several strategies to protect Your data such as:

a. Data loss prevention: We employ tools to ensure that Your data is not lost, accidentally deleted or stolen;
b. Firewalls: We use firewalls to monitor and filter network traffic, ensuring that only authorized users are allowed to access or transfer data.
c. Authentication and authorization: We use tools to ascertain and verify the credentials, assuring that user privileges are applied correctly; and
d. Endpoint protection: We use endpoint protection software to protect gateways to our network.

By using the Services or providing personal information to us, you agree that we can communicate with you electronically regarding security, privacy, and administrative issues relating to your use of the Services. If you have any reason to believe that your interactions with the Services are no longer secure, please notify us immediately at _____

22. Data Protection Impact Assessment

In the event that We change Our processes relating to data processing and protection, particularly through introduction of new technologies, We will undertake a risk assessment ("Data Protection Impact Assessment") to analyze the risk to Your data. This Data Protection Impact Assessment shall take into account the current nature, scope, context and purpose of data processing under this Policy, to flag any significant changes or risks to Your rights. If the risk level is found to be high even after undertaking standard risk mitigating measures, Our Data Protection Officer ("DPO") will contact appropriate statutory authority for consultation.

23. Data incident Notifications.

In cases where we are a data controller over data accessed in an unauthorized manner and such breach is likely to result in a high risk to the rights and freedom of a data subject, we will immediately notify the affected users directly and also notify the Commission within the statutorily stipulated period of 72 hours.

24. General Data Protection Rights for EEA, UK, Swiss Users.

We would like to make sure you are fully aware of all of your data protection rights. Every user is entitled to the following:

a. The right to access - You have the right to request copies of your personal data. We may charge you a small fee for this service.

b. The right to rectification - You have the right to request that we correct any information you believe is accurate. You also have the right to request that we complete the information you believe is incomplete.

c. The right to erasure - You have the right to request that we erase your personal data, under certain conditions.

d. The right to object to processing: You have the right to object to our processing of your personal data, under certain conditions.

e. The right to data portability - You have the right to request that we transfer the data we have collected to another organization, or directly to you under certain conditions.

f. If you make any request, we have **a month** to respond to you. If you would like to exercise any of these rights, please contact us.

The GDPR requires us to tell you about the legal ground we're relying on to process any personal data about you. The legal grounds for us processing your data include:

i. You provided your consent;

ii. It is necessary for our contractual relationship.

iii. The processing is necessary for us to comply with our legal or regulatory obligations; and/or

iv. The processing is in our legitimate interest to fulfill our service as an event organizing, content providing, and ticketing platform (for example, to provide you with customer service, and to protect the security and integrity of our systems, etc.)

25. For Nigerian Users.

We shall comply with the provisions of the Constitution of the Federal Republic of Nigeria 1999 (as amended), the Nigeria Data Protection Act 2023, The Federal Competition and

Consumer Protection Act 2019, Cybercrimes (Prohibition, Prevention) Act 2015, National Identity Management Commission Act, 2007, National Cyber Security Policy and Strategy 2021 and all other relevant laws, legislations and regulations in collecting, storing, using and sharing data of Users of our website.

26. For European Users

For European Users Data Protection Laws. If you are a resident of the European Union ("EU") or Switzerland, you are entitled to certain protections under the EU's General Data Protection Regulation ("GDPR") and/or other applicable laws (collectively, the "Data Protection Laws"), and this section applies to your use of the Services. As used in this section, the terms "processing," "processor," "controller" and "personal data" have the meaning given to them in the Data Protection Laws.

27. Dispute with Us

1. **Contact Us:** If you have a complaint about FKRO's privacy practices you should get in contact with our Data Protection Officer via_____. We will take reasonable steps to work with you to attempt to resolve your complaint.
2. **Time limit To Respond:** We try to respond to all legitimate requests **within 30 days**. Occasionally it could take us a longer period to process your request. If we require more time, we will inform you of the reason and extension period in writing. Please note that requests are subject to appropriate verification before processing.
3. FKRO and the disputing party shall seek to resolve the dispute amicably by using Alternative Dispute Resolution ('ADR') procedure acceptable to both parties before pursuing any other remedies available to them.

28. Complaint to Supervisory Authority

As part of exercising your data privacy rights against us, you can make a direct complaint to the **National Commissioner** under the **Nigerian Data Protection Act, 2023.** You can find the contact details here: _____

If you are a resident in the **EEA** and you believe we are unlawfully processing your personal data, you also have the right to complain to your local data protection supervisory authority. You can find their contact details here: https://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

If you are a resident in the **UK**, the contact details for the data protection authority is available here: dpo@ico.org.uk

If you are a resident in **Switzerland**, the contact details for the data protection authorities are available here: https://www.edoeb.admin.ch/edoeb/en/home.html

29. Contacting FKRO

If you have any further questions regarding our privacy policy, please contact us to let us know at: _____ and +234_____

This privacy policy was created on 01/12/2024