DATA PROCESSING AGREEMENT
(June 8th, 2023)

This Data Processing Agreement ("DPA") applies where there is no specific DPA submitted by the Controller towards Cira Apps which has been ratified by both parties and it will be updated over time as the applicable legal context evolves.

Cira Apps indicates the last date when this DPA has been updated at the top.

All changes apply and are automatically accepted by the parties (users and Corporate Clients) from the above posted date onwards, any conflicting clauses will supraceed the previous ones and new clauses constitute an addendum to the previous DPA version that has been automatically accepted by you at the date you started using Cira Apps services.

The parties to this DPA are:

Cira Apps Limited, established at **125 West Spoke Hill Dr, Unit B Wimberley, TX 78676**, United States (hereinafter called "the Processor" and also referred to as "we", "us")

and

The Corporate Client and its individual users who are utilizing Cira Apps tools (hereinafter called "the Controller" and also referred to as "you") while both also referred to as the "Parties".

Although the Processor has the knowhow to develop the tools (Apps) and inherent functionalities that the Controller and its users will be using, the Processor in fact acts under the instructions of the Controller in the sense that the Controller is the one which defines what Personal Data and pertaining to which Data Subjects as well as for which Purposes will be under Processing by Cira Apps tools.

This DPA, including its Annexes, bears the objective of defining and documenting a mutual commitment (by the Parties) towards the assurance of secure and confidential Processing activities with regards to Personal Data pertaining to 3rd Party natural persons (Data Subjects) who are either staff members; prospects or customer, in full compliance with the European Union Regulation 2016/679, General Data Protection Regulation (the "GDPR") plus other applicable Personal Data Protection Legislation, namely yet not limited), as per specific marketplace and country: CCPA (California U.S.); POPIA (South Africa); LGPD (Brazil); PDPA (Singapore) and APPI (Japan).

The Parties also hereby acknowledge to having entered into this agreement (a mutual commitment) by themselves as well as in the name and on behalf of their "Authorized Affiliates"/ "Partner" companies, towards which each Party resorts as an enabler of/

contributor to the enablement of Processor services in what implies the "Processing of Personal Data".

Both Parties agree therefore that GDPR is the "Personal Data" Protection Regulation which primarily rules on the entire herein described scope of Personal Data Processing Activities and inherent obligations since it bears, at present date, the most comprehensive and demanding set of rules and requirements towards the assurance of "Personal Data" Privacy, Security, and Confidentiality.

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by or is under common control with each Party. Whereas "**Control**," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the Party.

"**Controller**" as defined under the GDPR, means the Processor which determines the "Personal Data" that is forward to the other Processor under the "Services" scope, as well as the inherent "Processing of Personal Data" purposes, processes and/ or workflows which must be observed by the other Processor within the mutual relationship.

"**Data Protection Officer**"/ "**DPO**" as defined under the GDPR, means the natural person within a company/ organization (herein ahead referred to simply as "organization") who bear the responsibility of ensuring company compliance towards GDPR (as per defined under this Regulation), both by means of monitoring compliance status as well as acting towards the organization and management structure informing those about existing non-conformity points and the need for the organization to act upon them in order to make them compliant with GDPR rules, guidelines and requirements.

"**Data Subject**" as defined under the GDPR, means the identified or identifiable natural person to whom "Personal Data" pertains to. Both Parties understand that the "Data Subject" is the sole entity in full control of "Personal Data" which pertains to him/ her.

"**Data Subjects' Rights**" means the rights established towards the Data Subjects under the GDPR plus where applicable, the CCPA; POPIA and LGPD depending on the country of residence of the Data Subject.

GDPR means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the "Processing of Personal Data" and on the free movement of such data, while Repealing and replacing the Directive 95/46/EC from May 25th, 2018 onwards.

"**GDPR Training**" means the mandatory necessary endeavor which the Parties must undertake to ensure in a documented manner and as per GDPR requirements that their staff who performs "Processing of Personal Data" activities is fully aware of GDPR rules and guidelines.

"**IT Landscape**" means the set of IT assets and services of and at the disposal of each Party that enables their "Processing of Personal Data" operation, meaning the communications infrastructure (LAN, WAN, Wi-Fi networks), Data Center and technical rooms, Cloud-based services, workstations, software systems and tools, mobile devices in use, peripheral IT devices, Firewalls and web-based resources.

"**Legal Basis**" as defined under the GDPR, means the enlisted Legal Basis that an organization has to entice "Processing of Personal Data" activities under GDPR, namely (but not limited to) having documented: the "Data Subject'" Explicit Consent towards "Processing of Personal Data" activities; the organization Legitimate Interest in proceeding with "Processing of Personal Data" activities; accessory legal obligations that the organization must observe and which entitled it to proceed with "Processing of Personal Data" activities within the limits of such ruling and inherent obligations; other as per defined under GDPR.

"**Operational Landscape**" means the set of both Controller Operational Policies, Processes, Procedures, Workflows, permissions given to staff over the access to "Personal Data", 3rd Party under the scope of Corporate Client Core Business and related to "Processing of Personal Data".

"**Partner**" means any 3rd Party entity towards which each Party may resort in order to ensure "Processing of Personal Data" under a "Legal Basis" (as established by GDPR) and within the scope of agreed "Services". As determined under the GDPR these entities may act as Sub-Processors or Joint Controllers or still Independent Controllers in the case of the Controller.

Party means the companies that sign this DPA.

"**Personal Data**" as defined under the GDPR, means any data which by itself or when cross-referenced with other data enables one to univocally identify one given natural person, the "Data Subject".

"**Processing of Personal Data**" as defined under the GDPR, means any operation or set of operations which is performed on "Personal Data", whether or not by automated means, such as: collection/ retrieval; accessing (consultation, use); processing (organization, structuring, adaptation or alteration); storage (recording, erasure or destruction); sharing (disclosure by transmission, dissemination or otherwise making available, publishing).

"**Personal Data Breach**" as defined under the GDPR, means any "event" or "incident" (as per ITIL definition) which enables the accidental or unlawful

destruction, loss, alteration, unauthorized disclosure of, or access to "Personal Data".

Processor as defined under the GDPR, means the entity which proceeds with authorized "Processing of Personal Data" on behalf of the Controller and exclusively under the instructions of the Controller.

"**Services**" means the scope of "Processing of Personal Data" activities that are both inherent and/ or derive from the services being rendered by the Processor towards the Controller via its tools (the apps that Cira Apps has developed/ owns and are being used by the Controller.

"**Sub-processor**" as defined under the GDPR, means any 3rd Party entity engaged by the Processor or by the Controller to provide accessory services to the Processor while performing complimentary "Processing of Personal Data" within the scope of the "Services".

"**Supervisory Authority**" as defined under the GDPR, means an independent public authority that is established by an EU Member State pursuant to the GDPR which acts as the responsible public entity for auditing and enforcing local GDPR compliance.

2. PROCESSING OF PERSONAL DATA

a. "Processing of Personal Data"

The Parties commit to proceed with "Processing of Personal Data" activities in full compliance with the requirements of the GDPR including (but not limited to) having a defined and documented "Legal Basis" bearing each the sole responsibility for maintaining "Personal Data" in their possession Accurate, Secure and Confidential during "Processing of Personal Data" operations and observing defined retention periods.

The Legal Basis for "Processing of Personal Data" under the scope of the services from the side of the Processor is a Contractual Obligation that derives from Controller's using the tools.

The Processor commits not to undergo any Personal Data Processing activities which exceed or are not within the scope of the services, namely:

- Hosting and retention period that exceed the lifecycle inherent to the services;

- Access to Personal Data under the scope of the services by individuals or entities that do not play an active and relevant role in the fulfillment/ delivery of such services (staff or sub-Processors);

- Processing activities that exceed what is mandatory to enable the services;

- Sharing Personal Data under the scope of the services with unauthorized 3rd parties, meaning entities or individuals who are not relevant or required to enable the services fulfillment and delivery;

b. "Processing of Personal Data" Details

The subject-matter of "Processing of Personal Data" by the Processor exclusively pertains the agreed service scope as per the services and while exclusively aligned with the inherent "Legal Basis" of a Contractual Obligation by the Processor towards the Controller.

3. "DATA SUBJECTS'" RIGHTS

Both Parties commit to promptly inform each other (within 3 calendar days) upon the event of having "Data Subjects" exercising their rights towards them as per defined under the GDPR that may affect the other Party in the sense that action from it is required.

If and when feedback from or towards the other Party is required to address/ answer such "Data Subjects'" Rights request, both Parties hereby commit to ensuring full cooperation and making available required internal or "Partner" resources while bearing no cost towards the other Party.

4. PARTIES' STAFF

a. Confidentiality

The Parties will ensure to have established towards their staff, who are involved in "Processing of Personal Data", proper written confidentiality agreements (e.g. a data processing agreement under GDPR).

b. Limitation of Access

The Parties shall ensure that their staff' access to "Personal Data" is limited to those personnel performing relevant/ required internal operational tasks which contribute towards the execution of agreed "Services" and/ or which are done so under a "Legal Basis" towards the "Data Subject", further having set in place the appropriate access permissions that exclusively allow each staff member to

access “Personal Data” which is relevant under the scope of their individual contribution towards those “Services”.

c. “GDPR Training”

Both Parties commit to ensuring that their staff, who are involved in “Processing of Personal Data”, are trained on GDPR and properly informed about the requirements posed by GDPR, having documented the degree of acquired knowledge and awareness by their staff towards GDPR via an individual test.

d. Obligation to assist

Pursuant to Articles 32 to 36 of the GDPR, both Parties commit to mutually provide relevant and necessary assistance to the other Party where that does not comprehend a direct sole responsibility of one Party and it is relevant to ensure the observance of Personal Data Protection as well as the reply to any Supervisory Authority or a Data Subject exercising his/ her Rights under the law.

This includes also (as per article 28 of the GDPR), the obligation by the Processor to inform the controller if, under its perspective, a provided instruction infringes the GDPR ruling.

5. “SUB-PROCESSORS”

a. Appointment of “Sub-processors”

The Controller agrees that the Processor may resort to “Partners” that enable the provision of agreed Service which may also have to entice the “Processing of Personal Data” on behalf of the Controller and are, therefore its “Sub-processors” within this scope.

The Processor commits to having its Affiliates and Processors (sub-Processors before the Controller) entered into a written agreement containing data protection obligations not less protective than those in this DPA with respect to the protection of “Personal Data” to the extent applicable to the nature of the “Services” provided by such “Sub-processor”.

6. SECURITY

a. Controls for the Protection of Personal Data

Both Parties commit to implement and maintain (by regularly monitoring those) appropriate technical and organizational measures that ensure the Security, Integrity and Confidentiality of “Processing of Personal Data” while fully aligned with GDPR requirements as set forth in both

companies Privacy Policies and/ or Code of Conduct under and as per defined by GDPR.

7. PERSONAL DATA BREACH INCIDENT MANAGEMENT AND NOTIFICATION

Both Parties commit to maintaining security incident management policies and procedures specified in their Security, Privacy, Operational Processes and "IT Landscape" Documentation.

In the event of a "Personal Data Breach", with origin on the Processor, the Processor shall notify without undue delay the Controller after becoming aware of such "Personal Data Breach" when it relates to the Controller staff or any of its Clients/ Customers.

The notification process is described below under ANNEX 1.

8. PERSONAL DATA RETURN AND DELETION

Upon being informed by the Controller of the need to return or erase "Personal Data" under processing the Processor shall, to the extent allowed by applicable law, erase Personal Data in accordance with the market standards and best practices.

Appendixes List

Annex 1: Personal Data Breach notification

ANNEX 1

Personal Data Breach notification form

Personal Data Breaches (both potential as well as verified as effective) need to be reported by the Processor to the DPO of the Controller within 36 hours of having been detected, in writing to the contact email described in this document and containing details as per the bullet points below:

1. Nature of the personal data breach

a. insert a description of the breach including, how and when this occurred.
b. insert details of the categories and volume of personal data compromised.
c. insert details of the categories and volume of data subjects impacted.

2. Contact details

a. confirm contact details of the DPO or another individual responsible for compliance with the data protection who can be contacted in relation to the personal data breach.

3. Consequences of the personal data breach

a. insert a description of the likely consequences (from Processor's perspective) of the personal data breach for example identity theft, fraudulent activity, unauthorized access to accounts, etc.

4. Mitigation and containment

a. insert details of the measures taken or proposed to be taken to mitigate and contain the personal data breach and its effect, as well as to prevent it from happening again in the future.

This initial report will be followed by a final full and detailed version definite report from the Processor to the Controller 60 hours after the incident has been detected by the Processor.