AGREEMENT FOR THE PROCESSING OF PERSONAL INFORMATION/OPERATORS AGREEMENT

Full name of the **Service Provider**	**[THIRD PARTY SERVICE PROVIDER]** together with its successors-in-title and all subsidiaries, affiliates and assigns (hereinafter referred to as the "**Service Provider**")
Registration Number	[ADD DETAILS],
Physical Address	[ADD DETAILS],
Postal Address	[ADD DETAILS],
E-mail Address	[ADD DETAILS],
Effective Date	[ADD DATE] (hereinafter referred to as the "**Effective Date**")

For and on behalf of the Service Provider: (Who warrants that he/she is duly authorised)	
Date	
Place	
Signature	
Name	
Designation	

Full name of the **Customer/SYNAQ**	**SYNAQ (PTY) LTD.** together with its successors-in-title and all subsidiaries, affiliates and assigns (hereinafter referred to as the "**CUSTOMER**" or "**SYNAQ**")
Synaq Physical Address	Ballyoaks Office Park, Golden Oak House, 35 Ballyclare Drivel, Johannesburg 2021, South Africa
Synaq Postal Address	Ballyoaks Office Park, Golden Oak House, 35 Ballyclare Drivel, Johannesburg 2021, South Africa
Name	
Date	
Place	
Signature	
Name	
Designation	Information Officer
Email address	hello@synaq.com
For and on behalf of Synaq (Pty) Ltd. ("SYNAQ"): (Who warrant that they are duly authorised)	

(The Customer and the Service Provider, collectively referred to as the "**Parties**") **WHEREBY THE PARTIES AGREE AS FOLLOWS-**

1 **INTERPRETATION**

In this Agreement -

1.1 clause headings are for convenience and are not to be used in its interpretation;

1.2 unless the context indicates a contrary intention, an expression which denotes any gender includes the other genders; a natural person includes a juristic person and *vice versa*; and the singular includes the plural and *vice versa*;

1.3 words and expressions defined in any clause shall, for the purposes of that clause, bear the meanings assigned to such words and expressions in such clause; and

1.4 if any provision is a substantive provision conferring rights or imposing obligations on any Party, notwithstanding that it is only in a definitions clause, effect will be given to it as if it were a substantive provision in the body of this Agreement;

1.5 the following expressions bear the meanings assigned to them below and cognate expressions bear corresponding meanings -

1.5.1 "**Agreement**" means this document and annexures and addendums as agreed to from time to time in writing between the Parties, relating to the Protection of Personal Information;

1.5.2 "**Applicable Laws**" means any of the following, from time to time, that deals with the protection of Data Subjects Personal Information:

1.5.2.1 any statute, regulation, policy, by-law, directive, notice or subordinate legislation (including treaties, multinational conventions and the like having the force of law) (incl. but not limited to the POPIA);

1.5.2.2 the common law;

1.5.2.3 any binding court order or judgment;

1.5.2.4 any applicable industry code, policy or standard enforceable by law; or

1.5.2.5 any applicable direction, policy or order that is given by a regulator;

1.5.3 **"Confidential Information"** means any information of proprietary and confidential nature which has been or may be obtained by either Party from the other Party pursuant to the Relationship, whether in writing or in electronic form or pursuant to discussions between the Parties, including Personal Information;

1.5.4 "**Contract**" means any agreement and any annexures or schedules thereto, entered into between the Parties in respect of the provision of Services by the Operator to the Responsible Party, including any agreement in respect of fee estimates, scope of work and related assumptions;

1.5.5 "**Data Subjects**" means the Customer's affiliates, customers, Staff, and/or any other Person/s to whom Personal Information relates [Under GDPR a Data Subject is the same as under POPIA];

1.5.6 "**Disclosing Party**" means the Party disclosing Personal Information relating to Data Subjects, irrespective as to whether this Party is the Service Provider or the Customer;

1.5.7 "**Electronic Communication**" means any text, voice, sound or image message sent over an electronic communications network which is stored in the Version: 1.01 (31.10.2024) network or in the recipient's terminal equipment until it is collected by the recipient;

1.5.8 "**GDPR**" means the General Data Protection Regulations, as amended from time to time;

1.5.9 "**Information Officer**" means the Customer's registered Information Officer, as referred to in the Synaq (Pty) Ltd. Information Manual, compiled in terms of Section 51 of the Promotion of Access to Information Act 2 of 2002 [Under the GDPR a Data Protection Officer is appointed for these purposes];

1.5.10 "**Monitoring Device**" means any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or record any communication;

1.5.11 "**Operator**" means a person who processes Personal Information for the Responsible Party in terms of a contract or mandate, without coming under the direct authority of the Responsible Party [Under GDPR the Operator is referred to as "Data Processor"];

1.5.12 "**Parties**" means the Customer and the Service Provider as defined on the first page hereof or any combination of them as the contect may include and "**Party**" means any one of them as the contect may indicate;

1.5.13 "**Person**" means an identifiable, living, natural person or an identifiable, exisiting juristic person or any other person who is not a natural or juristic person;

1.5.14 "**Personal Information**" means information relating to any Person as defined under section 1 of the POPIA [Under GDPR referred to as 'Personal Data' and may be defined as any information that relates to an identified or identifiable ***natural person***, referred to as a "data subject."];

1.5.15 "**POPIA**" means the Protection of Personal Information Act 4 of 2013 (as amended);

1.5.16 "**Processing**" means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, as further defined in the POPIA;

1.5.17 "**Processing Limitations**" means the processing details as stated under Annexure B or such other limitations as may be agreed to from time to time in writing;

1.5.18 "**Regulator**" means the information regulator as defined in the POPIA or the regulator or information commissioner of the relevant European Memberstsate (in terms of the GDPR);

1.5.19 **"Relationship"** means the ongoing relationship between the Parties relating to, *inter alia*, the provision of Services by the Service Provider to the Customer in terms of Contracts or otherwise;

1.5.20 "**Responsible Party**" means a party who, alone or in conjunction with others, determines the purpose of and means for processing Personal Information, and who is also the Customer [Under the GDPR the Responsible Party will be referred to as the "Data Controller'];

1.5.21 **"Services"** means any supply or rendering of

services by the Operator for the Responsible Party in terms of a Contract and in terms of which the Operator inter alia Processes Personal Information of Data Subjects;

1.5.22 "**Security Standards**" means the security standards protocol agreed between the Parties in terms of a Contract. Where no standards have been agreed, the Service Provider shall conduct its Processing with reference to international standards / protocol for protection of Personal Information;

1.5.23 "**Staff**" means permanent, fixed term and temporary employees as well as subcontractors, agents, consultants, independent contractors and visiting students to the Service Provider and Customer who process Personal Information on behalf of the Service Provider or Customer, as applicable; and

1.5.24 "**Service Provider**" means the entity as defined on the first page hereof, that may also be fulfilling functions as an Operator.

2 RECORDAL

2.1 The Parties have engaged, or are about to engage, in the Relationship.

2.2 In the course of the Relationship and in any future interactions between the Parties, there is a likelihood that the Service Provider will receive, be exposed to and/or Process the Personal Information of the Data Subjects and that unauthorized processing of Personal Information could result in irreparable harm or loss to both the Data Subjects and the Customer.

3 EFFECTIVE DATE AND TERM

3.1 This Agreement shall commence on the Effective Date and shall remain in effect during the Processing of any Personal Information under any Contact and such period as agreed to specifically under this Agreement. The terms of this Agreement shall take precedence over any conflicting terms in such Contracts unless a Contract explicitly seeks to supplement or amend this Agreement.

4 SERVICE PROVIDER ACCOUNTABILITY

4.1 The Services Provider shall act as Resopnsible Party in the Processing of SYNAQ and its representatives Personal Information;

4.2 For all other Processing, the Service Provider shall Process Personal Information as Operator and will process Personal Information of Data Subjects (i) in connection with and for the purposes of providing the Services, and (ii) strictly in accordance with the Processing Limitations outlined in this Agreement or the Contract, or as specifically instructed or authorized by SYNAQ (acting as Responsible Party) in writing. The Service Provider will operate under the guidelines of POPIA and the GDPR.

4.3 The Service Provider acknowledges and agrees that the Customer retains all right, title and interest in and to the Personal Information and that the Personal Information shall constitute the SYNAQ's Confidential Information.

4.4 If the Service Provider is ever unsure as to the parameters or lawfulness of the instructions issued by SYNAQ, the Service Provider will, as soon as reasonably practicable, revert to SYNAQ for the purpose of seeking clarification or further instructions.

5 OBLIGATIONS OF THE SERVICE PROVIDER WITH RESPECT TO PERSONAL INFORMATION

The Service Provider shall –

5.1 only Process Personal Information in accordance with Applicable Laws, this Agreement and Customer instructions;

5.2 Adhere to SYNAQ's data privacy policies, Security Standards, and relevant industry regulations, ensuring full compliance with all Applicable Laws and regulations that apply to this Agreement.

5.3 at all times treat the Personal Information as strictly confidential;

5.4 not disclose Personal Information to any third party (including sub-contractors and Staff) except authorised Staff (see clause 9) or authorised Subcontractors (see clause 17);

5.5 ensure that all Staff and any other persons that have access to the Personal Information are bound by appropriate and legally binding confidentiality and non-use obligations which are substantially the same terms and conditions as outlined in this Agreement;

5.6 Implement reasonable technical and organizational measures (minimum standards outlined in **Annexure A**) to protect the integrity of Personal Information against unauthorized access, loss, or damage, considering:

5.6.1 any requirement set forth in law, stipulated in industry rules or in codes of conduct or by a professional body; and

5.6.2 generally accepted information security practices and procedures relevant to both the Service Provider and SYNAQ ;

5.7 In order to give effect to clause 5.6 above, the Service Provider shall take reasonable measures to:

5.7.1 identify foreseeable risks to Personal Information;

5.7.2 establish and maintain appropriate safeguards against the risk identified;

5.7.3 regularly verify that the safeguards are effectively implemented;

5.7.4 update safeguards in response to new risks and notify SYNAQ in writing about identified risks and implemented safeguards;

5.7.5 comply with reasonable auditing requirements set forth in this Agreement; and

5.7.6 agree to reasonable amendments to this Agreement from time to time, as required by data protection legislation for the benefit of Data Subjects.

5.8 SYNAQ may request written confirmation of compliance with these obligations, which the Service Provider shall provide within five days of receipt of such a request.

6 SECURITY COMPROMISE

The Service Provider must:-

6.1.1 **Immediate Notification**: Inform SYNAQ's Information Officer in writing within 24 hours upon becoming aware of any unauthorised use, disclosure, or processing of Personal Information. and comply with the following –

6.1.2 **Cost Responsibility**: Take necessary steps at its own expense to mitigate loss or compromise of Personal Information and restore affected information

systems promptly.

6.1.3 **Information Provision**: Provide SYNAQ with details within 24 hours regarding affected Data Subjects, the nature of the compromise, and, if known, the identity of the unauthorised individual involved.

7

7.1.1 **Regular Updates:** Report progress on resolving the compromise to SYNAQ at least once per business day until the issue is satisfactorily resolved.

7.1.2 **Required Notifications:** Where required by SYANQ, notify the Regulator as the case may be, affected Data Subjects, and such other authorities as required by law. Notifications must be in writing and include sufficient information for Data Subjects to take protective measures against potential consequences.

8 DATA SUBJECT REQUESTS AND REGULATOR REQUESTS

8.1 The Service Provider shall-

8.1.1 Fully cooperate with the Customer to address Data Subject requests for access, correction, deletion or complaints regarding Personal Information. Upon receiving a direct request from a Data Subject, notify the Customer in writing within 1 (one) business day.

8.1.2 under instruction and authority of the Customer, provide necessary assistance to fulfil its duties as Responsible Party relating to any requirement by the Regulator or Commissioner;

8.2 The Customer may disclose to a Data Subject that the Service Provider is involved in processing their Personal Information, notwithstanding confidentiality provisions.

9 SERVICE PROVIDER STAFF

9.1 The Service Provider shall:

9.1.1 **Restrict Access:** Limit access to Personal Information to staff who need it to provide services**,** and ensure staff only process Personal Information in accordance with this Agreement and are contractually bound to maintain its security and confidentiality, even after their engagement ends with the Service Provider.

9.1.2 Take reasonable steps to ensure that staff processing Personal Information receive adequate training on compliance with this Agreement and applicable data protection legistlation and regulations.

10 PERMITTED PROCESSING OF PERSONAL INFORMATION

10.1 The Service Provider shall only Process the Personal Information of Data Subjects under the following conditions –

10.1.1 **Specific Purpose**: Processing must be for a specific, lawful purpose and strictly in accordance with the Customer's written instructions. Any further processing requires prior written consent from the Customer, except for necessary actions to comply with legal obligations, as outlined in 11 shall apply;

10.1.2 **Respect for Privacy:** Processing must not infringe on the privacy rights of Data Subjects and must comply with relevant legislation regarding Personal Information.

10.1.3 **Engagement with Customer Only:** The Service Provider shall communicate solely with the Customer regarding Personal Information and may not disclose any details about processing to Data Subjects without prior written consent from the Customer through its Information Officer.

11 DISCLOSURE OR PROCESSING REQUIRED BY LAW, REGULATION OR COURT ORDER

11.1 In the event that the Service Provider is required to disclose or Process any Personal Information required by law, regulation or court order, or if the Processing of such Personal Information is required to enable a public body to properly perform a public law duty to carry out actions for the conclusion or performance of a contract to which the Data Subject is a party, is necessary for pursuing the legitimate interests of the Customer, a third party to whom the information is supplied, or a Data Subject, or complies with an obligation imposed by law on the Customer, the Sevice Provider will -

11.1.1 **Notify the Customer**: Advise the Customer through its Information Officer prior to disclosure if feasible; if not, notify immediately afterwards.

11.1.2 **Limit Disclosure**: Take reasonable steps to limit the extent of disclosure or processing.

11.1.3 **Opportunity to Intervene:** Provide the Customer a reasonable opportunity to intervene in proceedings if possible.

11.1.4 **Follow Customer Requests**: Comply with the Customer's requests regarding the manner and terms of disclosure or processing whenever feasible.

12 SEPARATION OF PERSONAL INFORMATION

Unless explicitly stated otherwise in this Agreement or any related agreements, all processing of Personal Information must be conducted separately from any data belonging to the Service Provider or third parties, ensuring no merging or combining of information occurs.

13 CROSS BORDER TRANSFER OF PERSONAL INFORMATION

13.1 The Service Provider must not transfer Personal Information outside the country in which SYNAQ has made available the Personal Informaiton without the SYNAQ's prior written consent.

13.2 If the Customer consents to a cross-border transfer, the Service Provider agrees to:

13.2.1 **Notify** SYNAQ**:** Provide details of the third party for inclusion in the processing limitations as per **Annexure B**.

13.2.2 **Ensure Compliance**: Ensure the third party complies with all obligations under this Agreement regarding Personal Information processing.

13.2.3 **Data Protection Standards:** Confirm that the territory of transfer has data protection laws comparable to POPIA and the GDPR, ensuring adequate privacy protections.

13.2.4 **Responsibility:** Remain responsible to SYNAQ for fulfilling all contractual obligations and be the sole

point of contact.

13.2.5 **Limit Further Transfers:** Prevent the third party from transferring Personal Information to other parties.

13.2.6 **Security Measures:** Ensure that the third party implements appropriate technical and organizational security measures (as per **Annexure A**).

14

14.1.1 **Binding Agreement**: Enter into an agreement with the third party that includes terms similar to this Agreement.

14.2 The Service Provider indemnifies SYNAQ against any claims or losses arising from breaches related to Personal Information processing by either the Service Provider or any offshore third party.

15 AUDIT RIGHTS OF THE CUSTOMER

15.1 SYNAQ or its agent may audit the Service Provider and its business processes or the processes of its sub-contractors (where authorized by the Customer) at any time with reasonable notice to ensure compliance with this Agreement regarding Personal Information protection and security. This includes access to systems, procedures, software, and physical security inspections. The Service Provider shall offer reasonable assistance and co-operation to SYNAQ and/or its auditors or inspectors in the carrying out of such auditing exercise.

15.2 To the extent that the Service Provider engages an independent auditor in relation to the provisions of applicable data protection legislation to carry out an audit of its operations, the Service Provider must provide copies of audit reports from independent auditors within seven days of completion.

15.3 If an audit reveals non-compliance, the Service Provider must rectify it promptly and provide written proof of correction to SYNAQ.

16 PERSONAL INFORMATION INDEMNITY

16.1 The Service Provider hereby indemnifies and holds harmless SYNAQ, its affiliates and their respective Staff, successors, cessionaries, delegatees and assigns, from any and all losses of both a patrimonial and non-patrimonial nature, all costs, expenses and damage, including consequential losses and damage as well as penalties and fines arising from the Service Provider's non-compliance with the provisions of this Agreement and any relevant data protection legislation.

16.2 Any limitation of liability set out in a Contract shall not apply to this indemnity.

17 SUBCONTRACTORS

17.1 The Service Provider may not sub-contract its obligations under a Contract where Personal Information as received from SYNAQ is Processed, without the prior written consent of SYNAQ.

17.2 Subprocessor changes. The Operator will inform SYNAQ of any addition or replacement of subprocessors and give SYNAQ an opportunity to object to such changes, provided that:

17.2.1 The Service Provider must inform SYNAQ of any new or replacement subprocessors and allow SYNAQ to object.

17.2.2 If an objection is raised, both parties will attempt to resolve it in good faith.

17.2.3 If unresolved, the Service Provider will provide services without the subprocessor or may terminate the service, allowing for a pro-rated refund.

17.3 Consent for subcontractors will depend on SYNAQ's risk assessment and audit requirements to ensure compliance with this Agreement.

17.4 Following the written approval by SYNAQ, all provisions of this Agreement apply to authorized subcontractors processing Personal Information, and the Service Provider remains responsible for their compliance. The Service provider shall update the Processing Limitations as per Annexure B to confirm the details of the sub-contractor.

17.5 The Service Provider undertakes to:-

17.5.1 Enter into written agreements with subprocessors to ensure they are bound by similar data protection obligations.

17.5.2 Supervise compliance with these obligations.

17.5.3 Ensure subprocessors implement appropriate technical and organizational measures.

17.5.4 Prevent subprocessors from modifying or combining Personal Information without prior agreement.

17.6 SYNAQ may verify compliance by:

17.6.1 requesting audits of third-party subprocessors;

17.6.2 confirming that such audits have been conducted.

18 RETENTION AND DESTRUCTION REQUIREMENTS

18.1 The Service Provider must adhere to SYNAQ's destruction and retention policies as outlined in Contracts, Security Standards, or communicated directives. Personal Information must be stored for the minimum periods specified by the Customer and destroyed according to established procedures.

18.2 Should any destruction instructions not be specified in a Contract or in the Security Standards when the Contract, in terms of which any Personal Information has been Processed by the Service Provider, terminates or expires, the Service Provider shall be required to timeously obtain written instructions from SYNAQ for the return and/or destruction of all such Personal Information in its possession.

18.3 Futher, at the request and option of the Customer (at any time during any Contract), and to its satisfaction, the Service Provider must promptly return or destroy all Personal Information in its possession.

18.4 Upon destruction or return of Personal Information, the Service Provider must provide a written statement confirming that no Personal Information has been retained.

18.5 The Service Provider shall comply with any request in terms of this clause 18 within 7 (seven) days of receipt of such request.

19 TRANSMISSION OF DATA

The Service Provider must ensure that all Personal Information communicated, including digital communications, is secured against unauthorized access. This requires implementing appropriate security safeguards in line with accepted information security practices and relevant industry regulations.

20 **APPLICABLE LAW**

This Agreement shall be governed by and construed in accordance with the law of the Republic of South Africa and all disputes, actions and other matters relating thereto shall be determined in accordance with such law.

21 **JURISDICTION**

21.1 The Parties consent and submit to the jurisdiction as agreed to under the Contract between the Parties.

21.2 Without prejudice to any other rights or remedies which SYNAQ may have, the Service Provider acknowledges that nothing herein shall preclude SYNAQ from seeking urgent relief or specific performance from a court of competent jurisdiction.

22 **NOTICES AND DOMICILIUM**

22.1 The Parties select as their respective *domicilium citandi et executandi* the physical address appearing on the first page for delivery of notices.

22.2 Any notice shall be deemed to have been given and received -

22.2.1.1 if posted by prepaid registered post, 7 (seven) days after the date of posting thereof;

22.2.1.2 if hand delivered, on the day of delivery; and

22.2.1.3 when Data Message (as defined under the Electronic Communications and Transactions Act 2002) has reached the information system of the recipient, unless otherwise proven.

22.3 Notwithstanding anything to the contrary contained in this clause 22, a written notice or communication actually received by a Party shall constitute adequate written notice or communication to it notwithstanding that it was not sent or delivered to its chosen domicilium citandi et executandi or in the manner provided in this clause19.

23 **WHOLE AGREEMENT**

23.1 Subject to clause **Error! Reference source not found.**, this Agreement constitutes the whole of the agreement between the Parties hereto relating to the subject matter hereof and the Parties shall not be bound by any terms, conditions or representations whether written, oral or by conduct and whether express or tacit not recorded herein.

23.2 No addition to, variation, consensual cancellation or novation of this Agreement shall be of any force or effect unless reduced to writing and signed by both Parties.

24 **ASSIGNMENT**

The Service Provider shall not be entitled to assign or otherwise transfer the benefit or burden of all or any part of this Agreement without the prior written consent of the Customer.

25 **WAIVER**

No waiver of any terms or conditions of this Agreement is binding unless expressed in writing and signed by the Customer. Any waiver is effective only for the specific instance stated. Delays or failures by the Customer to exercise any right, power, or privilege do not constitute a waiver, nor does a partial exercise preclude further or other exercises of rights or privileges.

26 **SEVERABILITY**

If any terms or conditions of this Agreement are deemed invalid, unlawful, or unenforceable, they will be severable, allowing the remaining terms to remain valid and enforceable. If an invalid term can be amended to make it valid, the Parties agree to negotiate a resolution.

27 **COSTS**

Each Party shall bear and pay its own costs of or incidental to the drafting, preparation and execution of this Agreement.

ANNEXURE A

People, awareness and training

- Employees with access to the Personal Information will sign an employment agreement to confirm confidentiality of Customer data.
- Regular awareness training on POPIA for all employees with access to the Personal Information.

Organisation control

- Internal data privacy policies and procedures which comply with requirements of POPIA.
- Data privacy is implemented and audited on compliance on an annual basis.

Physical security to Personal Information

- Access control in accordance with international standards.
- Locked cabinets, alternatively a locked offices, restricted to authorised personal, for where paper files are stored.

Security to Personal Information

- Encryption on communication of Personal Information.
- Anti-virus protection.
- E-mails are automatically scanned by anti-virus and anti-spam software.
- Firewalls.

Access control to Personal Information

- Employees are given access on a need to know basis.
- Access logging and control to Personal Information.

ANNEXURE B -

Processing subject-matter

[ADD DETAILS - The subject-matter is intended to establish the scope of the Operators Agreement. For example, the OA applies to processing in respect of issuing employee pay slips or managing employees' salaries and wages, or processing of personal information in relation to servicing a customer, OR customer details]

Processing duration

This agreement remains in place for the duration that the Operator provides services to Synaq and such time subsequent to expiration or termination that the operator may be in possession of Personal Information (as agreed to in writing)

Processing nature

The Operator is storing the information to [ADD DETAILS]

[DRAFTING NOTE: What is the operator doing with the personal information? For example, storing, collating, altering, destroying, or transmitting the personal information.]

Processing purpose

The purpose of the personal information received is to [ADD DETAILS]

[DRAFTING NOTE: It is important to describe the purpose of the operator's processing clearly. The operator must be made aware that no processing for purposes that do not fall within the explicitly defined purpose must occur. Purpose of the processing would be in terms of a contract or due to a statutory obligation. Please be specific, for example "employees' salaries and wages" and not simply "employment" purposes.]

Personal Information categories, processing areas and Data Subjects

Type of Data	**Description of data**	**Purpose of Processing**	**Data Subjects**
Personal Information	Data confirmed in the Agreement (i.e. domicile and contact persons detals)) VAT number Contact details	Conclusion of the Agreement Performance of Agreement Billing Purposes	Customer and its Authorised Users
Personal Information	As per Services	Execution of agreed Services	Authorised User and End User
Special Personal information	As per Services	Execution of agreed Services	End User
Children Information	As per Services	Execution of agreed Services	End User

Subcontractors/sub-processors:

[ADD IF APPLICABLE]