GLOBAL DATA PROTECTION POLICY

"URUP"

1. SCOPE AND INTRODUCTION

1.1. This document is intended to provide a policy under which URUP International Limited, its subsidiaries and affiliates and/or Navotron (Pty) Limited (hereafter for ease of reference only, termed "**URUP**") collect, maintain, secure and process information specifically focusing on personal information of individuals who interact with the URUP software platform.

1.2. **URUP** must collect information about individuals as part of normal business operations. The **URUP** Platform is used to host a series of online interactive components referred to as Journeys on behalf of clients, with the express goals of communicating and collecting information. The information collected may include *inter alia* Personally Identifiable Information such as *inter alia:*

- First Name
- Last Name
- Mobile / Contact Numbers
- Email Addresses
- Age

1.3. This policy intends to follow the data protection norms of the countries with the strongest protection Directives and Laws in which the **URUP** platform is operated.

1.4. Everyone has rights with regard to how their personal information is handled, and **URUP** recognises that the lawful and correct treatment of personal data is vital to our continued success in an increasingly regulated global marketplace. The processing of personal information (which is essentially any information which identifies a living individual) is an everyday activity for our business. During the course of our activities we collect, store and process personal information about our staff, suppliers, clients and our clients' customers; and we are committed to ensuring that it is treated in an appropriate and lawful manner.

1.5. **URUP** is based in Mauritius, however, we have operations in several other countries, including but not limited to the Republic of South Africa, the United Kingdom, Poland, Malaysia, Singapore, Australia and UAE.

1.6. Although this policy does not include the specific requirements of data protection law in each country in which we operate, its aim is to establish a uniform minimum standard which applies to all employees, contractors, distributors, sub-contractors, consultants, affiliates and business partners of **URUP** who handle personal information, irrespective of where they are based.

1.7. This policy does not form part of any employee's employment contract and we may amend this policy at any time.

1.8. We reserve the right to revise or supplement this Data Protection Policy from time to time at our sole discretion, and you agree to revisit this policy regularly at www.urup.com to ensure you are familiar with the most current version. By continuing to deal with us you will be agreeing to any such changes.

2. RESPONSIBILITY

2.1. It is the responsibility of all employees, contractors, distributors, sub-contractors, consultants, affiliates and business partners associated with **URUP** (together referred to as "Associate" in this policy) to ensure that this policy is understood and complied with.

2.2. This policy has been written by **URUP**'s legal team. Any questions or concerns about the operation of this policy should be referred in the first instance to the legal team.

3. WHEN DOES THIS POLICY APPLY?

3.1. This policy applies to the collection and processing of personal information.

3.1.1. What is personal information?

3.1.1.1. For the purpose of this policy, personal information (or personal data as it is referred to in certain countries in which we operate) is information which relates to living individuals who can be identified from that data, or from that data and other information to which we have, or are likely to have access.

3.1.1.2. Personal information is only gathered with your express permission, and can include a variety of things, such as names, addresses (physical or email), telephone numbers, and also more 'sensitive personal information' such as details about a person's age, gender, marital status, and opinions.

3.2. What is processing?

3.2.1. Essentially, any activity involving personal information will fall within the scope of 'processing'. This includes obtaining, recording, holding, using, disclosing, hosting, viewing or deleting personal information.

4. COLLECTION OF PERSONAL INFORMATION

4.1. In cases where **URUP** collects personal information and determines the manner and purpose for which it is processed, for example in our capacity as an employer, then we must ensure that we are open and transparent with the individuals from whom we are collecting data by providing them with certain information. This includes – the nature of the information being collected, the identity of the **URUP** entity collecting the data, our purpose for collecting the information and the purpose for which it will be used, whether the information is likely to be disclosed to any third parties, including overseas recipients (and if so, where those overseas recipients are based), the data subjects' right to request access and/or correction to their personal data and the contact details of the person to whom requests for access or correction should be sent.

4.2. Whilst it is not always necessary to obtain an individual's consent in order to process their personal information – consent can only be avoided in limited circumstances – and where possible we will always obtain the consent of the relevant individuals to any processing. If consent has not been obtained please speak to the legal team to understand whether any exceptions to the need for consent will apply.

4.3. In cases where we process personal information on behalf of our clients or other third parties, we rely on those clients/ third parties to ensure that when they are collecting the relevant information they notify the data subjects of how their data will be used and obtain the necessary consents to enable the data to be processed by **URUP** in the course of the provision of services.

4.4. The URUP Platform is designed to collect information from users who interact with journeys hosted on behalf of clients. The platform employs passive and active services to collect information from users.

4.5. The Platform collects information using one of three methods:

4.5.1. User Initiated Communications: via active services:

4.5.1.1. When users choose to interact with a journey hosted by the **URUP** platform via a Short Code Messaging Service or a USSD service the requesting telephone number will be recorded into the system.

4.5.1.2 The information will only be provided to a client if a user indicates in the journey that the client may contact the user.

4.5.2. User Initiated Communications: via passive services:

4.5.2.1. Passive services are services where a URL link in a journey is published and is free to access by any user. These services do not record information from a user through the passive service but may collect information from a journey.

4.5.2.2. Information will only be provided to a client if a user indicates in a journey that they wish to be contacted.

4.5.3. Client Initiated Communications:

4.5.3.1. Where clients provide a database of contacts to **URUP** the **URUP** platform can facilitate targeted communications to these individuals by generating a unique URL link for each user which allows the **URUP** Platform to collect information supplied by the client as soon as the user interacts with the URL.

4.5.3.2. URUP does not accept liability for accuracy of databases or contact details supplied by clients.

4.5.3.3. URUP will only accept a client-supplied database on the following terms:

4.5.3.3.1. The Client obtained the contact database legally;

4.5.3.3.2. The Client has ensured that all individuals who have unsubscribed or opted out of communications have been removed;

4.5.3.3.3. The information will only be provided to the client should the user indicate in the journey that they wish to be contacted.

4.6. Regardless of the collection method employed, the **URUP** platform requires each user to explicitly agree to terms and conditions governing the use of the platform services, and has an option to explicitly allow a client access to their personal information.

5. DATA PROTECTION PRINCIPLES

5.1. The following principles apply whenever **URUP** is processing personal information - whether **URUP** has collected that information or not, and irrespective of the country in which that processing takes place:

(a) Personal information must be processed fairly and lawfully - for personal data to be processed lawfully, certain conditions have to be met. The most common way of establishing compliance with this principle is to obtain the consent of the individual to whom the personal information relates. Where we do not obtain consent then there may be other provisions on which we can rely to show that we are processing information fairly and lawfully – these provisions vary dependent on jurisdiction – examples include where the processing satisfies a legal obligation of the processor (as opposed to a contractual obligation) or where the processing is necessary to enter into or carry out a contract to which the data subject is party. If consent has not been obtained please seek guidance from the legal team as to whether the processing is fair and lawful.

(b) Personal information must be processed for limited specified purposes - personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by legislation. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

(c) Personal information must be adequate, relevant and not excessive for the purposes for which it was collected – for example, we could not ask for or keep information about a client's religious beliefs, as this would not be considered relevant for the purposes of services we provide.

(d) Personal information must be kept accurate and up to date - steps should be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

(e) Personal information must not be kept for longer than is necessary - this means that data should be destroyed or erased from our systems when it is no longer required. However, please bear in mind that we may have certain legal obligations to retain data for specified time periods before we are able to destroy it. These legal obligations will mean that it is 'necessary' to keep the data for longer than we might otherwise require it.

(f) Personal information must be processed in line with data subject's rights - data subjects generally have a right to:

(i) request access to any data held about them by a data controller;

(ii) prevent the processing of their data for direct-marketing purposes;

(iii) ask to have inaccurate data amended; or

(iv) prevent processing that is likely to cause damage or distress to themselves or anyone else.

(g) Personal information must be kept secure - we must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental misuse, unauthorised access to, loss of, or damage to, personal data. We must put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data.

(h) Personal information should only be transferred to third parties where specifically permitted by the data subject – whilst there are some limited exceptions, in general we must ensure that we do not transfer personal information to a third party unless the data subject has consented to such transfer; and care must be taken to ensure that any third party recipient treats information transferred to it appropriately – this is usually achieved through due diligence and a written agreement between **URUP** and the relevant third party. (Pursuant to the Malaysian privacy laws it a requirement to keep and maintain a list of any disclosures to third parties).

(i) Personal information can only be transferred by **URUP** outside of the country in which it is collected in certain circumstances – as **URUP** is a global organisation this principle is particularly important to our business – we have therefore covered cross border transfers in more detail in paragraph 6 (six) below.

(j) Unique identifiers should be used with caution – we should only assign a unique identifier to an individual if it is needed in order to carry on our work efficiently, and we may not assign a unique identifier to an individual if the same identifier is used by another organisation.

6. CROSS BORDER TRANSFERS

Transfer or Transit-

6.1. Any action that allows data to be accessed or makes the data available, or potentially available, to someone outside of the country in which the data was collected could amount to a 'transfer'.

6.2. A transfer will not be deemed to have occurred if the data simply passes through another country on the way to a final destination unless some processing takes place in the other country en-route. In the context of the electronic transmission of data, this means that even though personal data may be routed through a third country on its journey from one country to another, this mere transit through a third country/ countries does not bring the transfer within the scope of the privacy legislation.

Case law in the United Kingdom has held that uploading personal data onto a webpage only constitutes a transfer to a third country if the relevant webpage is actually accessed by a person located in a third country. The process of merely uploading the data does not fall within the scope of the legislation. So, in the context of our business, if URUP Staff based in an office which is not in the country in which the URUP client is based can view personal information relating to that client, this will amount to a transfer. If a

client accesses our software from a third country and uploads information on to it, this will not amount to a breach of the principle as URUP is not accessing the information in a third country – the client is.

6.3. **Can information be transferred outside of the country in which it was collected?** The rules in each jurisdiction are different, and a brief summary is below. However, if you require specific advice regarding cross-border transfers please contact the legal team.

6.4 **Republic of South Africa:** Personal information may be transferred to an overseas recipient where at least one of the following applies:

(a) the recipient of the data is subject to a law or contract which provides for an adequate level of protection;

(b) the data subject consents to the transfer;

(c) the transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party, or the transfer is for the benefit of the data subject and:

(i) it is not reasonably practicable to obtain the consent of the data subject to that transfer, and

(ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

6.5. **Australia:** Personal information may be transferred to an overseas recipient where at least one of the following applies:

(a) the recipient of the data is subject to laws which uphold principles for the fair handling of the information and those laws are substantially similar to the Australian Privacy Principles (**APPs**);

(b) the individual consents to the transfer (noting that the organisation must, prior to receiving such consent, expressly inform the individual that if he consents to the overseas disclosure of the information, the organisation will not be required to take reasonable steps to ensure the overseas recipient does not breach the APPs); or

(c) a "permitted general situation" exists (this includes circumstances where disclosure is necessary to prevent a serious threat to life; where an organisation suspects unlawful activity; or where disclosure is necessary to establish or defend a legal or equitable claim)

6.6 **Hong Kong:** There are currently no restrictions for transfer of personal data outside of Hong Kong.

6.7 **Malaysia:** Under Malaysian privacy laws, personal data may be transferred to jurisdictions outside of Malaysia if any one of the following applies:

(a) the data subject has given his consent to the transfer;

(b) where the transfer is necessary for the performance of a contract between the data subject and the data processor; or

(c) where the data processor has taken all reasonable steps, and exercised all due diligence to ensure that the personal data will be processed in a manner which would not contravene Malaysian privacy laws.

6.8. **Singapore:** Transfer of personal data out of Singapore is allowed, provided that the transfer is made in accordance with the requirements of Singapore privacy legislation to ensure that a comparable standard of protection is accorded to personal data that is to be transferred overseas.

6.9. **United Kingdom:** Personal information may be transferred outside of the EEA if any one of the following conditions are met:

(a) the data subject consents;

(b) the European Commission has made a finding of adequacy in relation to the country to which the data is being transferred;

(c) the transfer is covered by standard contractual clauses approved by the European Commission.

7. DEALING WITH SUBJECT ACCESS REQUESTS

7.1. All individuals who are the subject of personal data held by **URUP** are entitled to:

7.1.1. Ask **what information URUP** holds about them and why;

7.1.2. Ask **how to gain access** to it;

7.1.3. Be informed how **URUP** is **meeting its data protection obligations**.

7.2. If an individual contacts' the company requesting this information, this is called a Subject Access Request.

7.3. Subject Access Requests from individuals should be made by email, addressed to info@urup.com.

7.4. **URUP** will verify the identity of anyone making a Subject Access Request before handing over any information.

7.5. In certain circumstances, the Data Protection Act governing the country of operation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, **URUP** will disclose requested data. However, **URUP** will ensure the request is legitimate, seeking advice from the company's legal advisers where necessary.

8. IMPLICATIONS OF NON-COMPLIANCE

8.1. If we place a client in breach of its obligations to its customers under privacy legislation, this may have serious commercial ramifications. These range from the imposition of penalties under the contract to its termination and civil action by the client for damages.

It will of course affect our reputation as well as our client's, and may therefore make it more difficult for us to secure new business.

8.2. If we contravene the privacy laws in the countries in which we operate (for example, in processing Associate data), the regulator may take enforcement action against us. This could result in financial penalties for our business. In some jurisdictions in which we operate, more serious contraventions could amount to a criminal offence and our directors could be found personally liable.

8.3. Non-compliance with this policy by URUP employees can result in serious consequences including disciplinary action, and potentially dismissal.

9. BREACH REPORTING

9.1. If you have any concerns in relation to data protection issues, you should immediately tell someone within our business. Contacting your line manager is the best place to start, but you can also contact the legal team. In all cases we undertake to treat details of individuals who report matters with the utmost confidence. This means that your identity will not be disclosed unless it is absolutely necessary to do so and no-one within our business should feel at a disadvantage in raising legitimate concerns.

10. REVIEW OF THE POLICY

10.1. We will regularly review the effectiveness of this policy to ensure it is achieving its stated objectives. Recommendations for any amendments should be reported to the legal team.