EUROPEAN UNION AND MEMBER STATES

GLOBAL DATA PROTECTION POLICY "URUP" – 2019-04-18

NO USERS UNDER SIXTEEN

IF YOU ARE UNDER THE AGE OF 16 YOU MAY NOT SUBMIT ANY INFORMATION TO URUP OR ANY OPERATOR OF THE URUP SOFTWARE

INDIVIDUALS WHO HAVE PREVIOUSLY ENGAGED WITH THE URUP SOFTWARE MAY ENQIRE, AMEND OR ANONIMYZE THEIR PERSONAL DATA ONLINE PROVIDED THAT THE SAME DEVICE THAT WAS USED TO ENGAGE PREVIOUSLY, IS USED..

---

1. SCOPE AND INTRODUCTION

This document is intended to provide a policy under which URUP International Limited, its subsidiaries and affiliates and/or Operators (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.
For the purposes of this document employees, contractors, distributors, sub-contractors, consultants, agencies, third party resellers, affiliates, business partners and any user of **URUP** that utilises the URUP Platform to collect and process information including personal information, irrespective of where they are based are collectively referred to as **"Operator"** or **"Operators"** where the plural applies.

1.1. Operators of the URUP platform may collect information about individuals as part of their normal business operations. The URUP Platform is used to host a series of online interactive components referred to as "Journeys" either created, published and managed by platform operators on behalf of clients, or directly by "Software as a Service" (SaaS) operators with the express goals of communicating and collecting information. The information collected may include Personally Identifiable Information such as:

1.1.1. First Name,
1.1.2. Last Name,
1.1.3. Mobile / Contact Numbers,
1.1.4. Email Addresses,
1.1.5. Age,
1.1.6. Gender, and
1.1.7. GPS Location,

but URUP and the platform's operators will not knowingly collect "sensitive Information" as defined in the European Union Global Data Protection Regulations (EU GDPR) and will not knowingly collect information from children below the age of 16 years.

1.2. This policy intends to follow the data protection regulations of the European Union as contained in the EU GDPR which take effect from 25 May 2018.

1.3. Every individual 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 many businesses. During the course of operator activities, the platform may collect, store and process personal information about staff, suppliers, clients and clients' customers; and URUP is committed to ensuring that these activities are treated in an appropriate and lawful manner.

1.4. **URUP** is based in Mauritius, however, we supply software platform services in several other countries, including but not limited to countries that are in the European Union but excluding the United States of America and associated Territories.

1.4.1 Although this policy does not include the specific requirements of data protection law in each country in which we operate, we comply with the EU GDPR and this Policy 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.

1.4.2 In the European Union URUP has appointed Data Protection Representative Limited as the company's Representative for purposes of the GDPR (http://www.dpr.eu.com):

1.4.3 All enquiries from individual EU Member State citizens or residents must be directed to the following email address: compliance@urup.com

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

1.6. This Policy shall form part of all agreements signed between URUP and Operators as well as Service Level agreements signed between URUP, Operators and Clients.

1.7. 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 interact with the platform regardless of which operator is currently hosting a journey you will be agreeing to any such changes

RESPONSIBILITY

1.8. It is the responsibility of all employees, contractors, distributors, sub-contractors, consultants, affiliates, SaaS purchasers and business partners associated with **URUP** (together referred to as “Operators” in this policy) to understand and comply with this policy.

1.9. 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 at eulegal@urup.com.

2. WHEN DOES THIS POLICY APPLY?

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

2.1.1. What is personal information?

2.1.1.1. 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 operators have, or are likely to have access.

2.1.1.2. Personal information is only gathered with your express permission, and can include a variety of details, such as names, email addresses, telephone numbers, age, gender and GPS Location, but shall not include ‘sensitive personal data’ as defined in the Article 9 of the EU GDPR (Regulation 2016/679).

2.1.1.3. In the European Union the URUP Platform may **not** be utilised to collect or process the following special categories of personal data: personal data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; or data concerning health or a natural person's sex life or sexual orientation.

2.2. **What is processing?**

2.2.1. Processing includes obtaining, recording, holding, using, disclosing, hosting, viewing or deleting personal information.

2.2.2 **URUP** is by nature a data processor and dependent upon specific circumstances or contracts with an operator or client or an end user URUP may also be a Data Controller or Joint Controller.

3. COLLECTION OF PERSONAL INFORMATION

3.1. Where **URUP** or an Operator collects personal information and determines the manner and purpose for which it is processed, the relevant entity or person is required to be open and transparent with the individuals from whom they are collecting data by providing them with certain information. This includes:

3.1.1. the nature of the information being collected;

3.1.2. the identity of the entity collecting the data;

3.1.3. the purpose for collecting the information;

3.1.4. the purpose for which it will be used;

3.1.5. whether the information will be disclosed to any third parties; including overseas recipients (and if so, where those overseas recipients are based);

3.1.6. the individual's right to request access and/or correction and/or deletion (pseudonymisation) of their personal data; and

3.1.7. the contact details of the person to whom requests for access or correction should be sent. Until 15 July 2018 this is: The Compliance Officer at compliance@urup.com.

3.2. **URUP** allows individual users that have previously interacted with the Software Platform to view, amend or delete personal information directly online if they are able to be positively identified from data on the platform.

3.3. **URUP** requires specific consent from individual persons to collect and process their personally identifiable information.

3.4. In cases where we process personal information on behalf of our clients or operators, we rely on those clients / operators to ensure that when they are collecting the relevant information, they inform the data subjects of how their data will be used and obtain the necessary explicit consent to enable the data to be processed by **URUP** in the course of the provision of data processing services.

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

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

3.6.1. User Initiated Communications: via active services:

3.6.1.1. When you choose to interact with a journey hosted on the URUP platform via a Short Code Messaging Service or a USSD service, the requesting telephone number will be stored transiently in your mobile phone or computer browser session and only saved permanently when you are presented with a Journey component that allows you to make a choice of whether you would like to share information with the Operator.

3.6.1.2. Information collected in this manner will only be recorded and made available with your express permission.

3.6.2. User Initiated Communications: via passive services:

3.6.2.1. Passive services are services where a URL link in a Journey is published and is free to access by any data subject capable of accessing the service or hosting platform. Information from a user through the passive service is not recorded by the URUP platform.

3.6.2.2. Information will only be provided to a client if you indicate in a Journey that you wish to be contacted.

3.6.3. Client Initiated Communications:

3.6.3.1. Where Operators provide a database of contacts to URUP the URUP platform may 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. This information is stored transiently in the data subject's browser session and only permanently recorded once the data subject is presented with a component allowing them to make an informed decision on whether they wish to share their information with the Operator or not.

3.6.3.2. URUP does not accept liability for accuracy of databases or contact details supplied by Operators.

3.6.3.3. URUP will only accept a Operator-supplied database on the following terms:

3.6.3.3.1. The Operator warrants that it obtained the contact database legally;

3.6.3.3.2. The Operator warrants that it has ensured that all individuals who have unsubscribed or opted out of communications have been removed from the database;

3.6.3.3.3. The information collected via a Journey originated by an Operator will only be provided to that Operator if the data subject indicates in the Journey that they wish to be contacted.

3.7. Regardless of the collection method employed, the **URUP** platform requires each data subject to explicitly agree to URUP's terms and conditions governing the use of the platform services and has an option to explicitly allow an operator access to their personal information.

4. DATA PROTECTION PRINCIPLES

4.1. The following principles apply whenever The **URUP** platform is used to **process** 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 URUP Platform will obtain the specific consent of the individual to whom the personal information relates prior to collection.

(b) Personal information must be processed for limited specified purposes - personal data may only be processed for the specific purposes notified to the individual 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.

(d) Personal information must be kept accurate and up to date – after 15 July 2018 individuals may view their current personal information if they have previously interacted with the URUP software and request amendment or deletion (pseudonymisation) of their data at any time provided that the same device is used to initiate the process. Up until 15 July 2018 all such requests must be directed to compliance@urup.com

(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 may mean that it is necessary to keep the data for longer than URUP might otherwise require it.

(f) Personal information will be processed in line with data subject's rights – an individual has a right to:

(i) access any personal data held about them by the **URUP** Platform**.**

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

(iii) amend inaccurate personal data and data-sharing choices online; or

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

(g) Personal information must be kept secure - URUP has appropriate security measures in place to prevent unlawful or unauthorised processing of personal data, and against the accidental misuse, unauthorised access to, loss of, or damage to, personal data. URUP has procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. **NOTE: Data and information accessed and downloaded for processing by Operators with the permission of a data subject is outside of the control of URUP and is not covered by the URUP platform security measures once it has. been downloaded by an Operator.**

(h) Personal information will only be transferred to third parties where specifically permitted by the individual data subject unless required by a competent legal authority. URUP will not transfer personal information to a third party unless the individual data subject has consented to such transfer.

(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) URUP will only assign a unique identifier to an individual if it is needed in order to carry on our work efficiently, and we will not assign a unique identifier to an individual if the same identifier is used by another organisation.

5. CROSS BORDER TRANSFERS
Transfer or Transit

5.1. 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 is defined as a 'transfer'.

5.2. 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.

5.3. Personal information may be transferred outside of the European Union Area 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.

6. DEALING WITH SUBJECT ACCESS REQUESTS

6.1. 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**.

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

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

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

6.5. In certain circumstances, the EU GDPR 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.

7. BREACH REPORTING

7.1. If you are a citizen of an EU Member State and you have any concerns in relation to data protection issues, you should immediately contact the URUP Representative: Data Protection Representative Limited at timbell@.dpr.eu.com with the subject heading "URUP".

8. REVIEW OF THE POLICY

8.1. We will regularly review the effectiveness of this policy to ensure it is achieving its stated objectives. Recommendations for any amendments should be made to the legal team at compliance@urup.com