



United Nations Population Fund
CO Ukraine
E-mail: ukraine.office@unfpa.org
Website: www.unfpa.org.ua

Date: April 16, 2021

Approved:

Jaime Nadal

DocuSigned by:
A blue ink signature of Jaime Nadal.
CD90116DD32D4D7...

Representative to Ukraine, United Nations Population Fund

REQUEST FOR QUOTATION

RFQ N° UNFPA/UKR/RFQ/21/02

Dear Sir/Madam,

The United Nations Population Fund (UNFPA) hereby solicits a quotation for the following services:

CREATION OF A MOBILE APPLICATION ON DOMESTIC VIOLENCE

This Request for Quotation is open to all legally-constituted companies in Ukraine that can provide appropriate services and have the legal capacity to supply/perform these services in Ukraine, or through authorized representatives.

About UNFPA

UNFPA, the United Nations Population Fund, is an international development agency whose mission is to deliver a world where every pregnancy is wanted, every childbirth is safe and every young person's potential is fulfilled.

UNFPA is the leading UN agency that promotes the right of every woman, man and child to a healthy life and equal opportunities. For more information on the Fund's activities, please visit the website: [UNFPA about us](http://unfpa.org/about-us).

I. Terms of Reference (ToR)

1. BACKGROUND

Violence is one of the largest human rights violations in the world. It has no social, economic, or national borders. Gender-based violence undermines the health, dignity, safety, and autonomy of its victims, but it remains hidden because of a culture of silence. It negatively affects the sexual and reproductive health of survivors.

Within the framework of its program aiming to prevent and combat domestic and gender-based violence, UNFPA, the United Nations Population Fund, launched in 2015 a national information and awareness raising campaign called Break the Circle. The title "Break the Circle" contains the following messages:

- domestic violence is repetitive;



United Nations Population Fund
CO Ukraine

E-mail: ukraine.office@unfpa.org

Website: www.unfpa.org.ua

- stereotypes, tolerance and ignorance of domestic violence are passed down from generation to generation;
- the courage of one survivor to get rid of violence inspires others to take this step.

Break the Circle campaign's website: <https://rozirvykolo.org>.

Facebook page: <https://www.facebook.com/rozirvykolo>.

The main message of the campaign: "Break the Circle - Violence is Not the Norm." All activities work to accomplish three tasks:

- disseminate information about available services for survivors;
- increase the level of recognition of violence;
- tell how to act in a situation of witnessing or/and being a victim of violence and to call for active action in these cases.

Achieving these three tasks is possible through the creation of the first mobile application in Ukraine (hereinafter the MA) for persons who have suffered from domestic violence or may find themselves in such a situation.

Goal

UNFPA Ukraine invites service providers who have successful experience in creating high-quality mobile applications and in advertising and promoting them. A short-term contract will be signed with the service provider according to which the service provider is expected to create and put into operation a mobile application. The selected service provider will be working under the direction of a Communication and Advocacy Specialist. The partner in creating the mobile application and the ultimate beneficiary is the Ministry of Internal Affairs of Ukraine (hereinafter the MIA).

2. OVERVIEW

The subject of development is a mobile application with a built-in hidden feature of calling for help.

The purpose of creating a mobile application

To provide possibilities for persons who may suffer or have suffered from domestic violence to quickly and safely seek help of the National Police of Ukraine.

"Quickly" means to use the possibility of communicating coordinates in a critical situation immediately and as accurately as possible (with/without the possibility of more detailed description of the situation).

"Safely" means to use the possibility of seeking help through the hidden useful feature of the mobile application.

The purpose of the mobile application:

1) To seek help in case of domestic violence:

- to have the possibility of sending a signal about the need for help to the manager console (the officer in the police station front office, 102 service);
- to have the possibility of receiving information on the location of the nearest police stations and other service providers involved in preventing and combating domestic violence (social services, hospitals) on the map;
- to have the possibility of receiving contacts of help services according to the geolocation.



2) To provide useful information on domestic violence:

- to set up a safety plan for survivors and an action plan for witnesses;
- to get a test to check the relationship for violence;
- to receive information on types and signs of violence.

MA's target audience is people over the age of 18 who use mobile phones with technical characteristics allowing them to download and use mobile applications.

Application language: Ukrainian.

Platform: iOS and Android.

Type of development: native.

Reference to successful interface of already existing mobile applications:

- Diya (which means Action in English)
- Monobank
- ZaTeb

3. MOBILE APPLICATION'S SPECIFICATION

3.1 Requirements for features of the mobile application

3.1.1 Blocks of the mobile application for general users

Functional requirements for general users of open and hidden parts of the MA are given in Table 1 below.

Table 1 - Functional requirements for general users

Blocks of mobile application for general users	
<i>block</i>	<i>description</i>
<i>open part of MA</i>	
open part of the application for receiving information	all features of the application are accessible except calls for the police
registration and authorization in the system to identify the user in the open part of the application	to enable the registration via Facebook or Google in order to save user's data
women's calendar	women's calendar containing ovulation/menstruation schedule
<i>hidden part of MA</i>	
registration and authorization in the system to identify the user	via id.gov.ua in order to call the police using the SOS button
the information block explaining how to use the MA	introduction to application (similar to MyPol application)
the alarm button to call the police	the possibility to display a button in the widget (disguised as a calendar on the desktop of the mobile platform) the integration of API with the Unified Information System of the MIA of Ukraine in order to make SOS call



the map with filters	location of police stations, social services, healthcare centers of Ukraine with information about opening hours, phone numbers, addresses the possibility to receive a geolocation, plot a route to a certain point on the map
Information Block I	containing phone numbers of other help services
Information Block II	the information block on domestic violence
the block integrated with the cloud storage	the possibility to instantly send a record of conversations, photos, videos to the application server
section about the mobile application	descriptive part of the application containing the information that the application is an official and alternative tool of communication with the National Police of Ukraine

Detailing:

The use of the MA is possible without registration and authorization, but with limited functionality (the open part of the MA: full access; the hidden part of the MA: map, Information Blocks I and II).

Upon registration and further authorization via id.gov.ua, when using the MA, access to the alarm button integrated with the UIS of the MIA of Ukraine is enabled in order to call the police.

The registration includes the following data:

- last name, first name (required), patronymic (optional);
- phone number;
- city of residence;
- residence address (optional);
- E-mail address;
- the request to access the geolocation of the application (allow);
- the request to access the mail (allow);
- notes (optional, any additional information the user wants to provide: blood type, Rhesus factor, availability of weapons, etc.);
- a consent as to the processing of personal data.

The registration is carried out using the integrated electronic identification system id.gov.ua (data for the integration is provided by the Customer).

The confirmation of the phone number for the possibility of SOS call (a password (automatically generated by the system and consisting of 4 digits) is sent to the phone number; a message can also be sent (for your safety, we recommend to delete this message).

For the authorization:

- The user can undergo the authorization procedure using one of the following ways:
 - o via id.gov.ua – for the hidden part of the MA
 - o via Facebook, Google – for the open part of the MA

The MA home page (the page which is displayed when the MA is launched) is the "women's calendar". In order to take advantage of the MA's hidden features, the user has to click on the displayed image (reference - ZaTeb application, Fig. 1).



After clicking on the image, the user goes to the hidden part of the MA. When using the MA for the first time, the introduction page is displayed which contains information on the necessity of the registration in order to access all features of the MA, namely the possibility to call for help.

The alarm button (reference - Kades application, Fig. 2) sends the information to the manager console containing the data provided by the user during the registration in the MA (including the user's actual geolocation).

As an option, the alarm button offers the possibility of sending additional information to the manager.

The map shows the location of all territorial bodies of the National Police of Ukraine, Centers of social services, hospitals and the user's location in relation to them. Additional features: plotting the route from the user's location to the nearest territorial body of the National Police of Ukraine and sending a message about the time the user has to spend to reach it (by walking, transport, public transport) (like GoogleMaps).

The block integrated with the cloud storage allows the user to take photos or record videos using the application, record a conversation (including a phone conversation) and send the information to the cloud storage. This feature is necessary to provide the possibility of documenting violence, threats, etc.

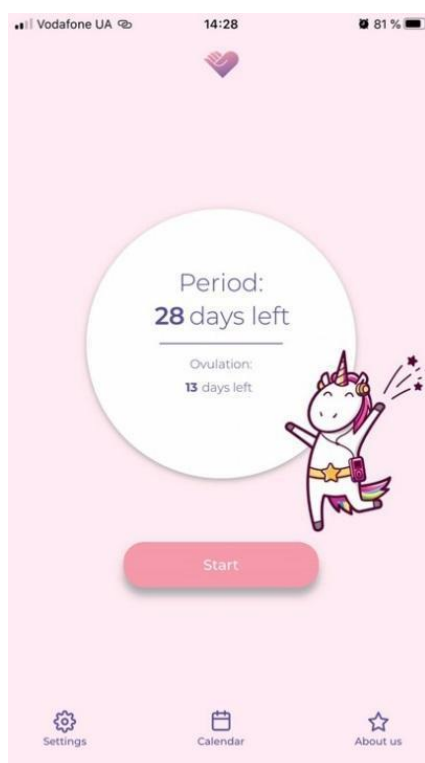


Figure 1

(the picture that redirects the user to the hidden part of the application is at the top middle of the screen)



Figure 2

3.1.2 Administrative blocks for managers

The descriptive part of the functionality for managers is given in Table 2 below.

Table 2 - Functional requirements for managers

Mobile application blocks for managers	
<i>block</i>	<i>descriptive part</i>
authorization in the system	authorization using a qualified electronic signature
map containing location of territorial bodies	the possibility to add locations on the map with their description: type of institution, name, address, phone number, opening hours
reporting the need for help	it is displayed on the map that shows the user's actual geolocation including processing statuses History and current calls with the following information: status of execution, reason of call, address, full name, phone number, coordinates, time and date of call, photo, video Current calls, statistics including information about call processing, reasons of call, call dynamics. The possibility to sort by date
notifications and messaging	feature for sending push messages
logging	a window containing the information on the authorization of the manager including a description of actions (login, change of status, creation of the publication) and time of event
feedback	for receiving messages with suggestions from application users
a window for user creation (administrator, manager)	new manager registration form and adding of management roles: managing calls, settings, notifications, receipt of messages, users banning, managing the communication with territorial bodies, feedback
users banning	blocking application users by phone number, e-mail, and a note about blocking



Detailing:

Interface for working with the desktop version of the application. Format: manager's administrative console.

Login to the administrative console using a qualified electronic signature, which will allow the customer and the administrator to identify the police officer and track the digital trace of actions in the MA.

When the alarm is received, the manager sees the location of the person who sent the alarm. Also, when appropriate alarm button is activated, the user's map opens showing the data that was specified during the registration.

In order to respond more effectively, it should be possible to determine the recurrence of calls, whether previous calls were confirmed/disconfirmed.

The operation of the MA interface and its desktop version should not require special skills, knowledge, technology or software products, except those needed for standard user work (download the application, login, use the application).

3.1.3 Additional features

Additional features must be implemented in the system:

- the possibility to run the MA offline (the open part of the application and information blocks);
- enabling the administrator to send push messages;
- quick exit button from the hidden part of the application;
- the possibility to view statistics (for the administrator).

3.1.4 Requirements for statistics (to be taken from the UIS of the MIA)

The MA should provide the possibility of obtaining statistical information:

- how much time a user spends on average and in which sections;
- how many users have downloaded the MA;
- on which platforms and in what quantity the MA is being downloaded;
- the number of registered and unregistered users;
- what features are used most often;
- how many users have used the alarm button.

3.1.5 Requirements for service components (to be taken from the UIS of the MIA)

Additional service components must be implemented in the MA:

- component for keeping directories and classifiers;
- component for visualizing analytical reports (diagrams, graphs, etc.);
- component for data backup and recovery;
- component for segment versioning and synchronization;
- component for the MA actions audit and logging.

3.1.6 Users' classes

I class: the guest is an unregistered and unauthorized user who has downloaded the MA on her/his phone.

The guest has the following rights:

- to be registered and authorized via Facebook, Google in the open part of the MA;
- the open part of the MA: to have access to the calendar and go to the hidden part;



- the hidden part of the MA: to be registered and authorized via id.gov.ua, to have access to the map, Information Blocks I and II.

II class: the user is a registered and authorized user.

The user has the following rights:

- to have full access to all MA features (except management and administration ones).

III class: manager is an officer in the police station front office.

The manager has a right to:

- have access to users' personal data;
- have access to users' geolocations;
- have access to the history of users' alarms.

IV class: the administrator is a person who provides technical support of the application on behalf of the customer.

The administrator has a right to:

- have full access to all MA administration features;
- have the possibility to send push messages to all users and guests;
- be allowed to edit any section;
- view statistics;
- prepare messaging;
- edit messaging;
- delete messaging.

3.1.7 Requirements for graphic design of MA

Style:

- compliance with the general style of the chatbot #ActAgainstViolence on Telegram including the addition of graphic elements for the brand book of the information and awareness raising campaign Break the Circle (in particular, purple color and elements of the circle and semicircle).

Transformation:

- 90-degree turn clockwise and counter-clockwise.

Additional requirements:

- utilization of contrasting color solutions;
- the MA should be as user-friendly as possible and understandable even to a child;
- a shift from one block to another is made by a finger slide (left or right);
- the main page of the MA's open part is the calendar, and the main page of the hidden part is the alarm button;
- possibility to navigate on all MA pages in its hidden part;
- permanent access to the registration/authorization (in the lower left corner).

There should not be a lot of text, flashing banners, dark and aggressive color solutions.



3.2 General requirements

The mobile application with the built-in hidden feature of calling for help is an integral part of the UIS of the MIA.

The MA must have architecture compatible with the UIS architecture.

The MA must have the following characteristics and meet the following functional requirements:

- to provide for interaction with the application server using the REST API, ensure compliance with the requirements for the client part;
- means should be provided for automated control of data integrity and consistency of stored information using cryptographic algorithms that prevent changes from being made during data exchange, including by the administrator;
- to provide mechanisms for the administration of users and their rights, as well as ensure the protection of personal data in accordance with current legislation of Ukraine;
- to provide the possibility to encrypt information, including information transmitted between the server and client by using methods that meet the regulatory requirements of the State Standards of Ukraine (DSTU), attested by a certificate of conformity or expert opinion of the State Service of Special Communication and Information Protection of Ukraine;
- the user's interface language should be Ukrainian by default with the possibility of quickly localizing the interface or separate functional subsystems and adapting them for English or other languages if necessary;
- the recommended data format during the exchange is JSON;
- to ensure work with physical devices of cryptographic protection and protected carriers of private keys which support interfaces of a smart card, SIM card and USB (diamond, crystal, SecureToken and others);
- to ensure the creation and generation of reports.

Performance requirements:

- the work of any script should not exceed 4 seconds;
- provided that the load on the server is not more than 20,000 per day.

Safety requirements:

- the transfer of personal data must be encrypted.

Reliability requirements:

- the system may be unavailable not more than 4 hours per year;
- MA reliability must be ensured by the UIS of the MIA.

3.3 Requirements for operation, maintenance, repair of the MA

The MA must be designed to operate as part of the software and hardware complex of the UIS of the MIA.

Technical and physical protection of MA hardware components, data carriers, uninterruptible power supply, reservation of resources, ongoing maintenance is provided by technical and organizational means offered by the UIS of the MIA.

3.4 Requirements for the technical support of the system

The MA should be implemented using the test and industrial environment of the UIS of the MIA.



3.5 Requirements for the information support of the system

Data storage levels in the MA should be built on the basis of modern relational DBMSs. Built-in DBMS mechanisms should be used to ensure data integrity.

Means of the operating systems and DBMS should allow for documenting and logging information processed in the MA.

The database structure should support the assignment of necessary access attributes and classification of information stored in accordance with current legislation of Ukraine.

Access to data should be provided to users taking into account their official powers and the category of information.

The technical means of the UIS of the MIA are used to ensure the storage of information.

The full data composition, their structure, methods of organization in the MA will be determined at the stage of detailed design.

3.6 System software requirements

The software to be used in developing the MA and code library should be widely distributed, publicly available and used on an industrial scale. Free and open-source software developed under free licenses (such as the GNU General Public License or BSD License) may also be used.

Microsoft Office, etc. should be used to document the system (texts, schemes, diagrams, etc.).

The MA software must be compatible with the software used by the UIS of the MIA.

Mobile platforms:

- Android, version 4.4 and higher;
- iOS, version 9 and higher;
- iPadOS, version 13.0 and higher.

Desktop Windows, version 7 and higher (for administrator and manager only). The web interface for the manager and administrator must work on the Internet Explorer v. 11+, Google Chrome latest version basis within the corporate network.

The MA must meet the requirements of the Marketplace (Google and Apple).

3.7 Requirements for integration and information interaction

The MA must:

- be integrated with the functional subsystems of the UIS of the MIA;
- be integrated with personal identification services (to be taken from the UIS of the MIA);
- be able to create scenarios of interaction with other systems, including the system of centralized management of patrol service units (abbreviated TSUNAMI System), which is a set of hardware and software, and the staff assigned to manage the assets of police mobile teams and includes interconnected blocks of 102 operator (service 102), manager, officer in the district police station front office.

A complete list of communication mechanisms and integration data will be determined at the stage of detailed design.



3.8 Information protection requirements

The information that will be stored and distributed in the MA will be of different levels of confidentiality. The MA will process the personal data of users, including the data that pose a particular risk to the rights and freedoms of data subjects (sensitive data).

Users should access the information stored in the MA in accordance with the functional needs and responsibilities, as well as rights of access to MA features.

Information about users who access MA features should be recorded and stored, such as date and time of access, the amount of data accessed, the purpose of and reasons for changing, viewing, transmitting and deleting data.

The user's access to the interface must have limited duration of the authorization session.

All exchange of information between components of the MA should be carried out using the application layer protocol with cryptographic libraries certified by the Administration of the State Service of Special Communication and Information Protection of Ukraine.

The interaction with web servers must be carried out via the https protocol (protection through SSL/TLS certificate).

3.9 Requirements for the protection against unauthorized access

Information protection in the MA is provided by creating an integrated information protection system (IIPS)/application of the security policy of the existing IIPS, which has been endorsed by state experts in the field of technical protection of information in accordance with current legislation of Ukraine.

The stages of creation of the IIPS/application of the security policy of the existing IIPS are agreed by the customer and supplier at the stage of detailed design.

In order to protect the information, the following measures should be taken:

- user identification and authorization using a login/password and/or qualified electronic signature (access to the information, except the open part of the MA, is provided only to identified and authorized users);
- request for re-authorization after the specified period or the absence of the user's active work during the work session;
- only one working session for one user;
- restriction and management of users' rights of access to MA resources;
- blocking of unauthorized access to hardware and software resources of the MA;
- protection of information integrity, transaction authenticity, transaction privacy, protection of the information against modification;
- information backup and recovery.

The MA provides for logging the following information:

- results of users' identification and authorization;
- results of information processing operations carried out by users;
- spoofing attempts to gain access to the information;
- changes made by MA administrators;
- facts of critical events in the system;
- facts of granting to users and denying them access to the information and processing rights.



United Nations Population Fund
CO Ukraine

E-mail: ukraine.office@unfpa.org

Website: www.unfpa.org.ua

The event logging should be done automatically. Registration data must be protected against the modification and deletion by users. Logging should be granted only to users who have security administrator rights, and for informational purposes only.

Registration of spoofing attempts to gain access to the information should be accompanied by a relevant notification sent to the security administrator.

The identification and authorization of users, granting and denying the right of access to the information contained in the MA should be done automatically.

The integrity of the software used to process the information should be monitored and no unauthorized changes should be allowed.

The software must monitor its integrity and report cases of detected attempts to make unauthorized changes.

There should be control over the integrity of hardware and software in order to protect the information. In the event of an attempt to violate their integrity, the processing of information in this component is suspended until the investigation of the incident is carried out.

3.10 Antivirus protection requirements

Requirements for the antivirus protection are set by regulations of the UIS of the MIA.

3.11 Requirements for modernization and development

MA's level of preparedness for changing the processes and management methods should be high, the system should provide the possibility of changing business processes and interfaces, and at least be able to further expand the modules and connect additional modules.

3.12 Additional requirements

Additional requirements for the MA may be determined at the stage of detailed design.

4. COMPOSITION AND CONTENT OF WORKS

Works on the creation and implementation of the MA are performed in stages (see Table 4).

Table 4 - Expected services and time frames

No	Name of stage	Description	Time frames
1	To create the mobile application	The mobile application must be developed in accordance with the terms of reference. Representatives of UNFPA Ukraine and the MIA will take part in approving the elements of the application.	The launch of the application's pilot version takes place no later than 4 months after signing the contract.
2	To perform application testing and its improvement	To provide testing of the mobile application by involving focus groups and making the necessary improvements to the interface or operation of the application.	The process of making identified changes must be completed no later than 5 months after signing the contract.
3	To transfer the mobile application for further technical support	The transfer of the application to the accounts of the State-Owned Enterprise INFOTEKH, Google, Apple Marketplace. Ensuring the transfer and deployment of the server part and API on the hardware of SOE INFOTEKH.	No later than 6 months after signing the contract.
4	To prepare and put MA into operation	To carry out procedures for purchasing goods, works, and services necessary for the creation of the IIPS/application of the security policy of the existing IIPS	No later than 7 months after signing the contract.



Requirements for the composition and content of works on preparing the automation object before putting the system into operation.

Requirements for the composition and content of works on preparing the automation object before putting the MA into operation will be determined at the stage of experimental operation.

5. TESTING PROCEDURES

Acceptance of the MA is carried out by the commission appointed by the MIA order.

The MA undergoes preliminary tests and experimental operation, which are carried out by the customer and the MA developer.

The MA testing is performed in accordance with the Testing Program and Procedures. The MA is tested for compliance of its parts with the Terms of Reference and operability. The results of the preliminary tests are recorded in the protocols on the results of preliminary tests.

Upon removal of shortcomings and modification of documentation, the certificate of MA acceptance in experimental operation is issued. The experimental operation of the MA is carried out jointly by persons designated by the customer and MA developer. The results of experimental operation are stated in the certificate of experimental operation completion. According to the results of experimental operation, the MA and documentation are finalized.

6. REQUIREMENTS FOR THE DOCUMENTATION

The design and operating documentation must contain the basic design and technical solutions for the creation and use of the MA. The composition and content of the documentation must meet the requirements of current legislation in the field of standard setting.

The language of the documentation is Ukrainian.

The MA documentation set must include:

- Terms of reference;
- Technical working project containing the following documents:
 - o Technical working project schedule
 - o Terms and definitions of basic concepts
 - o Explanatory note
 - o Organization structure description
 - o Automated features description
 - o General description of the system
 - o List of incoming data
 - o List of outgoing data
 - o Description of the data treatment technological process
 - o Description of the classification and encoding system
 - o Description of the information support
 - o Database directory
 - o Description of the information base organization
 - o Description of the set of software and hardware tools
 - o Equipment specification
 - o Drawings of the hardware



- Drawings of data centers' premises
- Cable pattern for external wires connection in data centers
- Operational procedures
- Operation instructions for the hardware package
- Operation environment scheme
- Testing program and procedures
- Testing certificate
- Form
- Certificate of acceptance in experimental operation
- Certificate of experimental operation completion
- Design and operating documentation set sufficient for creating the IIPS/application of the security policy of the existing IIPS, which contains a detailed description of protection mechanisms and organizational arrangements.

Payment

All services outlined in these terms of reference must be provided to the customer by November 30, 2021.

#	Services	Payment terms and conditions
1	Launching the application's pilot version and making the necessary changes after testing.	65% of the contract amount, after submission to and approval by UNFPA.
2	Testing the application, transferring the mobile application for further technical support, preparing and putting the MA into operation.	35% of the contract amount, after submission to and approval by UNFPA.

Intellectual Property

All information related to this project (documentary, visual, digital, cyber, project documentation, etc.) which the Contractor may deal with in the performance of its duties under this task shall remain the property of the United Nations Population Fund, which has exclusive rights to use it. Except for the purposes of this task, the information shall not be disclosed to the public or used in any form without the written permission of the United Nations Population Fund in accordance with national and international copyright laws.

II. Qualification requirements

UNFPA seeks a service provider with proven experience in developing mobile applications (examples of previously developed mobile applications, including description of goals and results).

The service provider should:

- be a resident entity of or have legal representation in Ukraine with respective official registration;
- have at least 2 years of experience in the area of software development and implementation;
- have experience in the field of video production and digital promotion; have experience as a designer (team) who worked on the visual component: examples of created UX/UI design;
- demonstrate ability to meet deadlines, work under pressure and measure results;



United Nations Population Fund
CO Ukraine
E-mail: ukraine.office@unfpa.org
Website: www.unfpa.org.ua

- be fluent in Ukrainian, Russian, and English.

Questions

Questions or requests for further clarifications can be submitted during the Kick off Meeting, which will take place on **April 26, 2021 at 11.00** via the Google Meet conference (a link to the conference will be provided later).

If you are going to participate in the Kick off Meeting, please send a confirmation containing the following information: company name, list of company representatives who plan to attend, and indicate their e-mail addresses to UNFPA contact person by **11:00 Kyiv time, April 23, 2021**.

Contact person:	<i>Nadiia Kovalevych</i>
E-mail address:	<i>kovalevych@unfpa.org</i>

If you cannot participate in the discussion, please send your questions and requests to UNFPA contact person (see Contacts in the Table above).

The deadline for submission of questions is **Thursday, April 29, 2021, 17:00 Kyiv time**.

III. Content of quotations

Quotations should be submitted in a single e-mail whenever possible, depending on file size. Quotations must contain:

- a) Technical proposal has to contain the information that would provide evidence for proposal evaluation due to the mentioned criteria, as well as information on a legal person. The Technical Bid must be submitted by electronic method of transmission at the e-mail address indicated in Section IV.
- b) The price offer submitted exclusively according to the corresponding form.
- c) Language of the proposal: English or Ukrainian.
- d) Technical Proposal and Price Offer should be sent in separate files and signed by the bidding company's relevant authority and submitted in PDF format.**

Instructions for submission

Proposals should be prepared based on the guidelines set forth in Sections III and IV, along with a properly filled out and signed price quotation form, and should be sent by e-mail only to the e-mail address of the contact person indicated below no later than: **Friday, May 07, 2021, 12:00 Kyiv time**. Proposals sent to any other address will not be considered.

Contact person:	<i>Iryna Bohun</i>
E-mail address:	<i>ua-procurement@unfpa.org</i>

Please note the following guidelines for electronic submission:

- The following reference must be included in the email subject line: **RFQ № UNFPA/UKR/RFQ/21/02**. Proposals that do not contain the correct e-mail subject line may be overlooked by the procurement officer and therefore not considered.
- The total e-mail size may not exceed **20 MB (including e-mail body, attachments, and headers)**. Where the technical details are in large electronic files, it is recommended that these be sent separately before the deadline.



Overview of Evaluation Process

The evaluation will be carried out in a two-step process by an ad-hoc evaluation panel. Technical proposals will be evaluated and scored first, **prior** to the evaluation and scoring of price quotations.

IV. Technical Evaluation

Technical proposals will be evaluated based on their responsiveness to the service requirements/ToR listed in Section I and in accordance with the evaluation criteria below.

Criteria	[A] Maximum points	[B] Points attained by Bidder	[C] Weight (%)	[B] x [C] = [D] Total points
Specific experience of company: <ul style="list-style-type: none"> <i>list of previous customers</i> <i>examples of previously developed mobile applications, including description of the goals and results</i> 	100		10%	
Expertise of the company related to the task: <i>history of the organization, general reputation, competence, and reliability</i>	100		20%	
Experience as a designer (team) to work on the visual component: <i>examples of created UX/UI design</i>	100		10%	
Experience of the team in building and integrating heterogeneous information systems: <i>examples of created integrations and systems</i>	100		25%	
Experience in working with law-enforcement agencies of Ukraine	100		5%	
Compliance of the declared working plan and methodology with the Terms of Reference	100		20%	
Quality of the prepared and submitted Bid materials	100		5%	
Confirmed experience of collaboration with international organizations <i>if such experience is available, a description of the work done and results must be provided</i>	100		5%	
Total amount	800		100%	

The following scoring scale will be used to ensure objective evaluation:

Degree to which the Terms of Reference requirements are met based on evidence included in the Bid submitted	Points out of 100
Significantly exceeds the requirements	90 – 100
Exceeds the requirements	80 – 89
Meets the requirements	70 – 79
Does not meet the requirements	0- 69



Only those technical proposals achieving the score of 70 points and above will be considered as qualifying for evaluation of the financial proposal.

Financial evaluation (maximum score: 100 points)

Financial proposals will be assessed based on their compliance with the financial proposal form. The maximum number of points (100) shall be scored to the lowest price proposal based on a special formula provided in the Terms of Reference. All other financial proposals will receive scores in inverse proportion according to the following formula:

Financial score =	Lowest quote (\$)	X 100 (Maximum score)
	Quote being scored (\$)	

Total score

The total score of each application will represent the weighted sum of its Technical and Financial proposals. The maximum score is 100 points.

Total score = 70% Technical score + 30% Financial score

- **Winner selection**

A contract for the period until December 31, 2021 between UNFPA and the supplier will be concluded with the bidder whose bid is the lowest and meets the requirements of the tender documentation.

- **Right to Vary Requirements at Time of Award**

UNFPA reserves the right at the time of award of contract to increase or decrease by up to 20% of the volume of services specified in this RFQ without any change in unit prices or other terms and conditions.

- **Payment Terms**

The payment will be made in accordance with the acceptance by the Customer of above deliverables (results of the work), as well as based on complete set of invoice supporting documentation.

The payment will be made in currency: Ukrainian Hryvnias. In case of two currencies involved, the United Nations Operational Rate of Exchange should be used on the day UNFPA instructs that payment(s) (web: www.treasury.un.org).

Terms of payment are 30 days upon receipt of transport documents, invoices and other documentation required by the contract.

- **Fraud and Corruption**

UNFPA is committed to preventing, identifying, and addressing all acts of fraud against UNFPA, as well as against third parties involved in UNFPA activities. UNFPA's policy regarding fraud and corruption is available here: [FraudPolicy](#). Submission of a proposal implies that the Bidder is aware of this policy.

Suppliers, their subsidiaries, agents, intermediaries, and principals must cooperate with the UNFPA Office of Audit and Investigations Services as well as with any other oversight entity authorized by the Executive Director and with the UNFPA Ethics Advisor as and when required. Such cooperation shall include, but not be limited to, the following: access to all employees, representatives, agents, and assignees of the vendor; as well as the production of all documents requested, including financial records. Failure to fully



United Nations Population Fund
CO Ukraine

E-mail: ukraine.office@unfpa.org

Website: www.unfpa.org.ua

cooperate with investigations will be considered sufficient grounds to allow UNFPA to repudiate and terminate the Agreement, and to debar and remove the supplier from UNFPA's list of registered suppliers.

A confidential Anti-Fraud Hotline is available to any Bidder to report suspicious and fraudulent activities at [UNFPAInvestigationHotline](#).

- **Zero Tolerance**

UNFPA has adopted a zero-tolerance policy on gifts and hospitality. Suppliers are therefore requested not to send gifts or offer hospitality to UNFPA personnel. Further details on this policy are available here: [ZeroTolerancePolicy](#).

- **RFQ Protest**

Bidder(s) perceiving that they have been unjustly or unfairly treated in connection with a solicitation, evaluation or award of a contract may submit a complaint to the UNFPA Program Manager Olesia Kompaniets at e-mail: kompaniets@unfpa.org. Should the supplier be dissatisfied with the reply provided by the UNFPA Head of Unit, the Bidder may contact the Chief, Procurement Services Branch at procurement@unfpa.org.

- **Disclaimer**

Should any of the links in this RFQ document be unavailable or inaccessible for any reason, bidders can contact the Procurement Officer and request them to share a PDF version of such document(s).



PRICE QUOTATION FORM

Name of Bidder:	
Date of the quotation:	
Request for quotation No:	RFQN^o UNFPA/UKR/RFQ/21/02
Currency:	UAH
Validity of price quotation: (The quotation shall be valid for a period of at least 3 months after the submission deadline)	

PRICE QUOTATION FORM

No	Description	Number of Staff	Hourly Rate	Number of hours worked	Total
• Professional Fees					
<i>Total Professional Fees</i>					UAH
• Out-of-Pocket expenses					
<i>Total Out-of-Pocket Expenses</i>					UAH
Total Contract Price, excl. VAT (Professional Fees + Out-of-Pocket Expenses)					UAH
Total Contract Price, incl. VAT (Professional Fees + Out-of-Pocket Expenses)					UAH

I hereby certify that the company mentioned above, which I am duly authorized to sign for, has reviewed **RFQ No UNFPA/UKR/RFQ/21/02 (CREATION OF A MOBILE APPLICATION ON DOMESTIC VIOLENCE)**, including all annexes, amendments to the RFQ document (if applicable) and the responses provided by UNFPA on clarification questions from the prospective service provider. Further, the company accepts the General Conditions of Contract for UNFPA and we will abide by this quotation until it expires.

Name and title	Date and place



United Nations Population Fund
CO Ukraine
E-mail: ukraine.office@unfpa.org
Website: www.unfpa.org.ua

Annex I:

General Conditions of Contract:

De Minimis Contracts

This Request for Quotation is subject to UNFPA's General Conditions of Contract: De Minimis Contracts, which are available in: [English](#), [Spanish](#) and [French](#).