unicef | for every child

TERMS OF REFERENCE

for the Corporate Contract for the provision of
Services (digital platform) for engagement of participants in the Milky Way Race 2022

Service:	**Milky Way Race virtual challenge Software-as-a-Service (SaaS) solution implementation, deployment, and support services**
Supervisor:	**Žana Hinek**
Duration:	**09.05. – 31.12.2022.**
Location:	**online**

I. Background

With the objective of carrying out Croatia CO's 6th UNICEF Race to raise awareness about UNICEF's mission and activities in the country, as well as raise funds for UNICEF programs, increase visibility among the targeted population (individuals between 25-55 years of age) and offer an engagement opportunity to existing and new donors, the Country Office requires the procurement of services from international company specialized in implementation and deployment of IT platform to support virtual event.

The need for this type of event was identified within the CO program cycle 2017–2022, and the learnings gained through the past events will be used to create the 2022 event. This activity supports our 2017-2022 CPD and 2017-2022 PSFR Strategic Plan, while also combining sports-related events with solidarity and engagement of citizens for the benefit of children.

To accomplish these goals, UNICEF will conduct market research to identify a qualified virtual event organizer with the required experience (both in software development, know-how in organizing virtual races and technical and marketing support).

II. Purpose of the Contract

As the sport events landscape is deeply influenced by Covid-19 pandemic, and major public gatherings are cancelled or limited, the concept of the annual sport event was thoroughly reengineered to comply with social distancing practices and measures imposed by the National Crisis Headquarters. Therefore, the concept of a virtual race was introduced in 2020 and repeated in 2021, and with the uncertainty of the epidemiological situation in the Fall, Croatia CO's CMT decided to continue with the organization of virtual event exclusively. In line with this, a virtual event SaaS all-in-one platform needs to be fully adjusted and customized to meet the Country Office's programmatic, advocacy and fundraising goals.

III. Objective of the Corporate Contract with expected results/outcome/products/sub products/outcomes

The general objective is organizing virtual sport event which includes Software-as-a-Service (SaaS) solution that can replicate physical event and fundraising needs into all-in-one platform.

Agreed Services:

Software-as-a-Service (SaaS) solution provider agrees to provide the following services to UNICEF CO Croatia:

1. To provide access to mobile application based virtual challenge for the end-users for activities such as but not limited, to running, walking, or cycling.
2. To feature UNICEF CO Croatia on the Platform as the entity to whom financial support will be provided during the Challenge with the goals of promoting and marketing UNICEF CO Croatia and UNICEF CO Croatia's work, creating and expanding visibility for UNICEF CO Croatia and UNICEF CO Croatia's cause.
3. To feature the Sponsors on the Platform as entities supporting UNICEF CO Croatia during the Challenge with the goal of providing brand visibility and credibility to Sponsor's corporate social responsibility and philanthropic efforts.
4. To feature Corporate Teams on the Platform as entities supporting UNICEF CO Croatia during the Challenge with the goal of providing brand visibility.
5. To develop and publish content on the Platform in collaboration with UNICEF CO Croatia, as determined in service provider discretion with input and timely responses from UNICEF CO Croatia, to feature UNICEF CO Croatia and Sponsors during the Challenge.
6. To manage and address technical issues with the Platform that arise during the Challenge.
7. To develop a support service workflow, in coordination with UNICEF CO Croatia, to distribute the workload among UNICEF call center (as 1st level support) for non-critical problems and service provider's technical team (as 2nd level support).
8. To create and facilitate a training session with UNICEF CO Croatia call center team.
9. To provide FAQ guidelines to UNICEF CO Croatia call center team so they can handle all usability "1st level" support questions.
10. To create a document to outline what the "2nd level issues" are that could prevent someone from participating therefore allowing UNICEF CO Croatia call center team to focus on resolving 1st level support questions and distribute the workload among service provider's technical team and UNICEF CO Croatia call center team.
11. To support UNICEF CO Croatia in providing excellent customer support by focusing on resolutions and response time of issues or reported incidents. Providing UNICEF CO Croatia with insight into this support by centrally administering shared document or a dashboard with up-to-date information on:
    - Date of report
    - Issue description
    - Username experiencing issues
    - Screenshots/video of the problem
    - Status of resolution (reported, currently investigated of fixed)

Best option is to define a Service Level Agreement (SLA) where the contractor would assist in development and set up of necessary elements to deliver optimal problem-solving framework.

12. To provide information and analytics to UNICEF CO Croatia on the progress of the Challenge as well as a final statistic report (number of users, teams, shared posts, shared comments, kilometers collected etc.) and a final analytic report (the most "liked" photo/post, the most active users, detailed analytic for the sponsors' teams, the app usage frequency analytics, most reported bugs and dysfunctionalities, etc.).
13. To offer access to contact information and data (such as images posted by the End Users on the Platform), as determined by service provider in its sole reasonable discretion, to UNICEF CO Croatia, subject to any permissions, settings, or other limitations offered to End-Users through the Platform, and subject to the requirements of applicable law related to disclosure of such information.
14. To provide reasonable technical and project management support to UNICEF CO Croatia in furtherance of the Services.

Agreed functionalities of the Platform:

1. Online fundraising tool to allow Milky Way community to sign up to virtual challenge and invite their friends, family, and companies to do the same.
2. Options for virtual community building by creating teams, sharing photos and communication content.
3. Customization and storytelling options to enable spread the awareness, share beneficiary stories, and give sponsors visibility on mobile application and virtual challenge dashboard, in terms of corporate logotype placement, pinned posts and photo filters.
4. Usage of service provider's mobile application tracking options and enabling registering for unlimited activity types (running, walking, cycling, etc.).
5. Virtual challenge dashboard and mobile application completely customizable in the Milky Way look and feel.
6. Set up donation button within the mobile application, leading to UNICEF domain donation website.
7. Mobile application 3rd party integrations with world-known sports applications like Strava, Fitbit, Garmin, pedometers, Health apps, etc., that all sync with the click of a button and in-app GPS tracking.
8. Individual and team leaderboards for individual or team competitions.
9. Options for digital community building with customizable options for selfie photos taken, chats, comments, and social media sharing.
10. Global engagement enabled by mobile application (no geographical limitations for participation).
11. Integrated sponsorship opportunities: registration website, pinned up posts, mobile application.

Agreed terms on IT Security:

1. Applicability / Scope

The security requirements outlined in this document are mandatory and apply to any internal or external party who is providing a solution, a system or a service to UNICEF which processes, stores or transmits information that meets the classification criteria reflected in this document.

1.1. Class I System Properties

A defining property of a Class I system is as follows: a system / service(s) which processes and or stores personal data or confidential UNICEF data or is linked to a critical business process(es), as defined in this section.

Personal data

UNICEF defines personal data similar to article 9 of the EU general data protection regulation 2016/679 (GDPR): "Data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Profiling data when there is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."

Any system that processes and or stores personal data is a Class I system.

Confidential UNICEF data

Information such as, but not limited to, sensitive Program Division Reports, HR Records, investigative documents, etc. Any system that processes and or stores confidential UNICEF data is a Class I system.

Linked to a critical business process

The input received during this phase, shall be viewed as "initial", and will require follow-up consultation with the office of Business Continuity prior to the system / solution becoming an operational asset (placed into production). Any system that is linked to a critical business process shall be classified as a Class I system.

2. Security Requirements

All the requirements covered in this area reflect controls that shall be included in any Request for Proposal (RFP), Work Orders / Package, Term of Reference (ToR) or any document that may be used by a service provider or professional services entity which are providing UNICEF a "Product" or "Service". Both business owner (data controller) and the service provider (data processor) share the obligations for ensuring proper implementation of the requirements.

It shall be noted that the requirements outlined in this section be viewed as an additional layer to complement vendors existing security eco system and not a replacement. In cases where a service provider's controls are more restrictive the service provider's controls shall prevail and be formally captured by both parties.

2.1. General Security Requirements

a) UNICEF shall reserve the right to assess the quality and accurateness of outsourced software development and operational maintenance of the system / application, whether it be through security assurance testing or through external security assessment.

b) Solution / Service shall be protected from unwanted network traffic by network filtering or separating measures that lay outside of the system, such as externally controlled routers and firewalls.
c) The system shall have proper end-point protection, with the following minimum requirements:
• malicious code protection measures
• host firewall configured utilizing, at a minimum, least privileged access controls (services, user, communication access).

2.2. Validation of Security Controls
a) UNICEF shall reserve the right to periodically validate the implementation of the security requirements outlined in this document via:
• Security Assurance Testing
• Vulnerability Testing
• Penetration Testing
• Audits
• On-site checks

2.3. Compliance & Certifications
a) Any vendor that provides hosting of any class I system, shall carry, at a minimum ISO2700K, certification and provide the following documents for view: ISO Certification, SoA, SOC 2, and SOC3 audit findings.

2.4. Identification, Authentication and Authorization
a) The service provider shall follow the principle of least privilege, guaranteeing that users, group, role, and device identifiers will be unique, assigned to each entity (user or process). Each application user role shall have a correspondent database connection according to its privileges.
b) The service provider shall centrally manage the user account using federated identities and whenever possible integrate their solution with the UNICEF Identity Management System. In case authentication is password based; the password shall forcefully adhere to the common best practice quality requirements and will be forcefully renewed frequently. The allocation of authenticators will be controlled and management through a formal process.
c) Multi-factor authentication will be used for:
• privileged accounts and
• user access outside of UNICEF trusted network.
d) All the user and system accounts shall be disabled after a defined period of inactivity, in accordance with organizational standards. All default accounts and or passwords shall be removed or changed. Approvals will be required for creation, deletion or modification of any account.
e) All access from external networks will traverse specific entry and exit points where external communication is terminated and re-established into a UNICEF controlled ICT ecosystem.
f) Account lockout features will be used for invalid authentication attempts.
g) Application code shall never contain any credentials.

2.5. Availability and Deletion

a) Systems availability shall be set according to Service Level Agreements, to meet the Confidentiality, Integrity and Availability requirements commensurate with its classification, as noted above

b) Any deletion of confidential / personal data must be done so that it cannot be reconstructed.

2.6. Cryptography

a) The system shall have cryptographic controls in place to secure sensitive data while in transit, while at rest and while in use. At a minimum, UNICEF cryptographic standards shall be used. In cases where vendor cryptographic standards exceed published organizational standards, vendor technical controls shall prevail.

b) Personal data shall be masked, pseudonymized or otherwise protected from unauthorized access.

c) The service provider shall use best practice or industry standard secure data exchange protocols and keep them up to date, as per defined UNICEF standards. Outdated and / or compromised protocols shall never be used.

d) All passwords shall be encrypted with best current practices or strong industry standards cryptographic algorithms and secure keys. The keys will be generated using strong cryptographic algorithms.

e) Key files must be protected from unauthorized modification using an application that enforces automatic reconciliation from an authoritative source.

f) Encryption keys shall be securely stored outside of the systems on which they are used.

2.7. Secure Development

a) The system shall be engineered following the 'security by design' principles.

b) The system shall be developed following the 'data protection by design and by default' principle. Hence appropriate technical and organizational measures shall be in place to implement the data protection principles and safeguard individual rights. Data protection shall be integrated in processing activities and operational practices, from the design stage throughout the solutions lifecycle.

c) Development and tests of the system will be done with fictitious or pseudonymized information.

d) Any source code developed specifically for the system shall undergo a security assurance testing, and business impact analysis to bring operational business to acceptable level. Risk tolerance level shall the established by the system / solution owner.

e) Access to program source code and associated items - such as designs, specifications, testing and validation plans - shall be strictly controlled; to prevent the introduction of unauthorized functionality.

f) The system shall display generic error messages that do not disclose detailed information such as process logs, account or system information.

g) Executable code will not be implemented on an operational system until evidence of conforming to the testing criteria (user approval, QA, or the equivalent) is acquired and the associated program source libraries have been updated.

2.8. Updating assets' inventory

a) The assets' inventory related to UNICEF applications shall be updated, as part of the operational process, capturing all system elements, describing their business function, location / identifiers and business owner.

2.9. Security Operations

a) The system shall be hardened, which means that:

• only the services and network ports necessary for efficient operation are up and running

• all application code is patched and kept up to date and

• limiting the accounts and removing, changing or disabling default accounts and passwords

Note: In order to ensure proper risk driven methodology is followed, patches shall fall into one of the following categories, which are classified by the application / system vendor.; critical, noncritical. The patching window SLA, shall be formally documented by both vendor and UNICEF's Designated Authority (D.A.).

b) Servers and applications shall be configured to run with the minimum system authorizations necessary. The service provider shall ensure the implementation of the appropriate technical and organizational measures.

c) The system must be configured to display generic error messages that do not disclose detailed information such as process logs, account or system information.

d) The production environment shall be separated from the test and development environments. preferably on logically and physically different systems.

e) Development and test environment shall have the same patch level as the production environment.

f) The production environment shall not have any development tools.

g) Configuration/Application source code/customized work, shall be protected from unauthorized access / modification and reside in non-production environment with proper back-up / resiliency policy.

h) The system shall have malicious code protection measures. Logs generated by malicious code protection measures shall be monitored.

2.10. Vulnerability Management

a) The service provider is required to run security tests. Test will run prior to the launch of the system and periodically afterwards; with a minimum frequency of once a year.

b) The service provider is required to report on the results of the security scans and the remediations taken. These reports will be sent to UNICEF's Chief of IT Security or the relevant focal point(s).

c) Critical security patches shall be applied within 3 days, following established testing / change management processes.

2.11. Change Management

a) Any changes to UNICEF system(s) or software shall be agreed upon between ICT and the business division / office owner of the affected system and third party.

b) Changes to system and/or application post baseline will be documented (version / build number),

along with description via a formal change management process. The service provider shall report the following information about patches, at a minimum: type, version, reason, post test results after implementation. Patches that fail testing will also be recorded and documented.
c) The updating of the operational software, applications and program libraries will only be performed by trained and qualified administrators upon appropriate management authorization.

2.12. Log Management and Monitoring

a) The system shall generate and process auditing tracks covering all actions taken on personal data, including data access only.
b) Authentication validation activities and all changes in authorization shall be logged and securely stored, with limited access.
c) Access to content, key information and or any modifications to operational program libraries shall be logged and restricted.
d) Logs and events will be generated in a format that can be easily parsed and used as an input for logging process management.
e) Integrity log checking shall be performed to ensure consistency.
f) The system, application, as well as underlying services and or networks, shall be monitored and activities logged.

2.13. Security Incident Management

A security breach, shall be viewed as:
• a failure in security controls which leads to the accidental, unlawful or unauthorized access, destruction, loss or alteration of data / information that processed / stored on system
• a failure in security controls which leads to the accidental, unlawful or unauthorized access to ICT resources, such as - but not limited to - computing resources (processing and or storage / services) and communication resources (infrastructure).
a) Security breaches shall immediately be communicated to UNICEF's Point of Contact.
b) A security incident notification and escalation procedure shall be formally documented and contractually enforced between the service provider, and UNICEF's Security Operations Centre.

3. Agreed terms on Intellectual property

1. No provision in this Agreement shall be construed as an assignment or transfer of ownership of any copyrights, patents, trade secrets, trademarks, or any other intellectual property rights from service provider to UNICEF CO Croatia.
2. Service provider only grants UNICEF CO Croatia a limited license to use its intellectual property to the extent necessary to provide the Services, and for UNICEF CO Croatia to use the Platform for its intended purpose. This license is limited to the term of this Agreement and is non-exclusive, non-modifiable, and non-transferable.
3. UNICEF CO Croatia only grants service provider a limited license to use the content provided by UNICEF CO Croatia to the extent necessary to provide the Services. This license is limited to the term of this Agreement and is non-exclusive and non-transferable.

IV. Deliverables (delivery dates and/or details of how the work should be delivered)

1. UNICEF CO Croatia develops event project plan and timeline.
2. Service provider appoints dedicated project manager to lead the process of setting up a virtual race.
3. Service provider delivers set of documents with pre-defined specification to guide UNICEF CO Croatia through the process of customization:
   a) Setting up the challenge
   b) Challenge Template
   c) Challenge Communication Content
4. Service provider delivers set of documents with pre-defined specification.
5. Service provider provides online training to guide UNICEF CO Croatia call center support team through the process of support.
6. Upon delivery of all necessary elements pre-defined in customization documents, service provider creates customized virtual challenge no later than August 8, 2022.
7. Service provider performs Set up and maintenance of the web dashboard excluding ticketing.
8. Service provider performs Set up and maintenance of the mobile application.
9. Service provider ensures corporate sponsor customizable elements of mobile application.
10. Service provider ensures creation of 50 corporate teams, pre-set in the app.
11. Service provider ensures 4 filter for selfies provided by UNICEF.
12. Service provider ensures in app communication - 4 "pinned post" in total during the challenge
13. Service provider performs Project Management and Technical Support throughout virtual challenge Monday – Friday.
14. Service provider performs additional technical support on 2 weekend (4 days) peak days.
15. Service provider ensures Weekly check in with your Dedicated Project Manager.
16. All customized elements of virtual challenge registration website and mobile application should be approved by UNICEF CO Croatia prior to publishing.
17. It is expected for Contractor to perform tasks in accordance with the Project Plan and in compliance with UNICEF's policies and mission.

V. Performance indicators for evaluation of results

1. Tasks handled and executed in timely manner, as per event project plan.
2. Dedicated service provider's project manager that leads UNICEF CO Croatia in setting up a virtual challenge through regular e-mail updates and attending recurring online meetings.
3. Set of documents with pre-defined specification to guide UNICEF CO Croatia through the process of customization explained in detail and delivered prior to creating official creative agency briefs.
4. Set of documents with pre-defined specification to guide UNICEF CO Croatia through the process of 1st level support.
5. Respecting support reporting and resolution time mutually specified in advance.
6. Virtual challenge customized and set-up within ten (10) days upon delivery of set of documents on customization.
7. Customized elements of the virtual challenge pre-approved by UNICEF CO Croatia.
8. All tasks performed in accordance with the Project Plan and in compliance with UNICEF's policies and mission.

VI. Qualifications and experience required

1. Established expertise and experience in virtual race organizing (required knowledge, specific skills, specialists, experience)
2. Software-as-a-Service solution advanced features to support UNICEF CO Croatia fundraising, programmatic and advocacy goals
3. Capabilities and resources to carry out required tasks
4. Human resource capacities to carry out required tasks in specified timeframe
5. Excellent team coordination and management.

VII. Definition of supervision arrangements

Contractor will be supervised by the UNICEF Corporate Fundraising Officer, Žana Hinek, through participation in meetings or through exchange of information on progress and activities via phone and e-mail as necessary.

VIII. Duration of the contract

Duration: 09.05. – 31.12.2022.

IX. UNICEF resource in case of unsatisfactory performance

If the Services or Deliverables provided by the Contractor do not conform to the requirements of the Contract or are delivered late or incomplete, without prejudice to any of its other rights and remedies, UNICEF can, at its option:

1. by written notice, require the Contractor, at the Contractor's expense, to remedy its performance, including any deficiencies in the Deliverables, to UNICEFF's satisfaction within thirty (30) days after receipt of UNICEF's notice (or within such shorter period as UNICEF may determine, in its sole discretion, is necessary as specified in the notice),
2. require the Contractor to refund all payments (if any) made by UNICEF in respect of such non-conforming or incomplete performance,
3. procure all or part of the Services and/or Deliverables from other sources and require the Contractor to pay UNICEF for any additional cost beyond the balance of the Fee for such services and Deliverables,
4. give written notice to terminate the Contract for breach, in accordance with Article 6.1. below, if the Contractor fails to remedy the breach within the cure period specified in Article 6.1. or if the breach is not capable of remedy,
5. require the Contractor to pay liquidated damages as set out in the Contract.

X. Support provided by UNICEF

UNICEF Office for Croatia, as well as other partners working on this event, will provide support as required.