

**AGREEMENT
CONCERNING THE PROTECTION OF PERSONAL DATA
OF REFUGEES AND ASYLUM-SEEKERS
BETWEEN
THE OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR REFUGEES (UNHCR)
AND
xxxxxxx**

Preamble

Whereas registration is an important protection tool, including protection against refoulement, forcible recruitment, and for ensuring access to basic rights: family reunification, assistance, and to implement appropriate durable solutions;

Whereas, in carrying out its mandate, UNHCR conducts the registration of refugees and asylum-seekers in the country, subject to the availability of resources and to the Office's operational needs;

Whereas every person has a right to be protected against the arbitrary or unlawful interference with his or her privacy and for the protection of personal data. This includes ensuring that personal data:

- shall be obtained and processed only in fair and lawful ways;
- its use should be specified and authorized by the person concerned
- it should only be limited in detail for a specific purpose and
- accurate and, where necessary, kept up to date;

Whereas effective co-operation between UNHCR and its partners and commercial services suppliers involves the exchange of refugees and asylum seekers' personal data for the provision of services compatible with UNHCR's international protection mandate;

Whereas sharing, electronically or otherwise, of personal data of refugees and asylum-seekers by UNHCR with partners and commercial suppliers providing services to refugees and asylum seekers must be subject to data protection safeguards, including the consent of the persons concerned;

Whereas the sharing of personal data should not compromise the Office's humanitarian and non-political character, jeopardize human rights or undermine the climate of trust and confidence which needs to exist between the Office and persons approaching it for protection and assistance;

Whereas pursuant to the Frame Agreement (the "Contract") entered into with xxxxxxx renders services which incorporate processing personal data of refugees and asylum seekers on behalf of UNHCR;

Now therefore, UNHCR ("the "Data Controller") and xxxxxx (the "Data Processor"), collectively referred to as "the Parties", agree as follows:

Article 1

Definitions

1.1. For the purpose of this Agreement the following definitions shall apply:

Data Subject means the refugees or asylum-seekers who are the beneficiaries of medical treatment in the context of the services provided by the Data Processor and persons to whom the Personal Data refers.

Personal Data means any personal information including identifying information defined under Article 3 below of whatever nature and in any format or media that, by whatever means, is provided to the Data Processor by the Data Controller, is accessed by the Data Processor on the authority of the Data Controller or is otherwise received by the Data Processor on the Data Controller's behalf and includes transactional or other information associated with the Data Subject generated by the Data Processor in the course of providing the service to the Data Controller.

Processing in relation to Personal Data , includes the obtaining, recording or holding of such data or carrying out any operation or set of operations on the data, including organization, adaptation, or alteration; disclosure by transmission, dissemination, or otherwise; and alignment, combination, blocking, erasure, or destruction.

Services means the specific activities for which the Data Controller has engaged the Data Processor as set out in the Annex xxxx to the Contract).

Country means Lebanon;

Registration record status means the processing status of an individual with reference to the Data Controller's registration record for the country: the registration record status is "active" if the person to whom the record relates is a refugee or asylum-seeker and remains in the country, or "closed" if the person concerned has been determined not to be in need, or no longer in need, of international protection, or has died or has moved other than temporarily to another country.

Article 2

Purpose of personal data transfer

- 2.1. The purposes of transferring personal data is to enable the Data Processor to perform its Services (under the Contract) as follows:
- (a) Identifying beneficiaries under the Data Controller's mandate who are in need of medical treatment;
 - (b) Providing the identified beneficiaries and/or the Data Controller with the following services in Lebanon:
 - Validating medical entitlements: ascertain whether the Data Subject is entitled to health care as per the Data Controller protocols: - compile a monthly report of cases by name, refugee registration number (proGres Individual ID), age, sex, and validity of claim.
Enrolment: enroll those with a valid entitlement to proceed for consultation with a health care provider.
Pre-treatment approval: pre-approve treatment and medical procedures before commencement of treatment except in those special cases where, if treatment is not provided, the risk of death or serious complications are imminent.
 - Peer review: ensure attending physicians adhere to approved treatment protocols and guidelines; choose conservative, least expensive and effective treatment procedures.
Audit bills: audit and scrutinize medical bills and ensure accurate billing of medical procedures, consultation, supplies, and consumables are properly itemized and charged.
 - Hospital bills: submit a dossier of bills to the Data Controller (or its partner as per instructions subsequently notified in writing by UNHCR) for payment.
- 2.2. The Data Processor warrants to process the Personal Data strictly in accordance with the purposes as stated above in the manner specified from time to time by the Data Controller; and for no other purpose or in any other manner except with the express prior written consent of the Data Controller;

Article 3

Personal Data elements to be transferred

- 3.1. The Data Controller shall share with the Data Processor the following personal data of each Data Subject registered by, or having filed a refugee status claim before, the Data Controller in Lebanon upon that person's consent and for the specific and limited purpose of providing the services set out in Contract and Article 6 below:
- UNHCR ProGres Case Number;

- UNHCR generated individual ID;
 - Names (Last Name, First Name, Mother Name);
 - ID picture;
 - Country of Origin;
 - Date of birth;
 - Gender;
 - Current address (i.e. Governorate level);
 - Family size;
 - The relationship to the Principal Applicant (e.g. wife, son, daughter, mother etc.);
 - Vulnerability status (i.e. limited to severely vulnerable or not).
- 3.2. The Data Controller shall share with the Data Processor any corrections or updates made to the personal data already shared in accordance with paragraph 1 of this Article 3.
- 3.3. Requests by the Data Processor for the disclosure by the Data Controller of the personal data of any Data Subject beyond that defined in Article 3.1 shall be considered by the Data Controller on a case-by-case basis, taking into account the Data Processor's legitimate interests in obtaining such information for the performance of the Services, and only upon consent of the Data Subject concerned.
- 3.4. The request must be made in writing and must clearly state the reasons why disclosure is necessary and the purpose for which the data is requested.

Article 4

Means by which Personal Data Are Shared

- 4.1. Personal Data will be accessed directly in 'RAIS', and, in certain circumstances, can be transferred by UNHCR in an electronic format. The electronic format may be an Extensible Markup Language (XML), Portable Document Format (PDF), an Excel spreadsheet, or a word-processing document. Access would be limited to authorized users delegated by the Partner and restricted to the necessary relevant data.

Article 5

Confidentiality of Personal Data

- 5.1. The Data Processor shall take all necessary measures to ensure that the personal data of Data Subjects is handled only by authorized personnel, whose use and access is required in the context of the performance of the Services. The Data Processor shall take all necessary measures to ensure that such use and/or access is audited through

an AAAA "Authentication, Authorization, Accounting and Auditing" compliant computerized system. In accordance with article 13 of the General Conditions of Contract (Annex xxxxx to the Contract), the Data Processor shall regard the Personal Data as confidential data and not disclose such data to any person other than to employee, agents or sub-contractors to whom disclosure is necessary for the performance of the Services and subject to paragraph g) below or except (subject to Article 6.2) as may be required by any law or regulation affecting the Data Processor. Under no circumstances shall personal data shared under this Agreement be disclosed to third parties and specifically with the country of origin of the Data Subjects concerned.

Article 6

Data Processing and Security of Personal Data

6.1. The Data Processor warrants that it will:

- a) Process the Personal Data in accordance with the terms and conditions set out in this Agreement and where the standards imposed by the data protection legislation regulating the Data Processor processing of the Personal Data are higher than those prescribed in this Agreement, then in accordance with such legislation;
- b) Implement appropriate technical and organizational measures to safeguard the Personal Data from unauthorized or unlawful processing or accidental loss, destruction or damage in compliance with best industry standards, having regard to the state of technological development and the cost of implementing any measures, such measures shall ensure a level of security appropriate to the harm that might result from unauthorized or unlawful processing or accidental loss, destruction or damage and to the nature of the Personal Data to be protected;
- c) Implement technical and organizational measures to procure the confidentiality, privacy, integrity, availability, accuracy and security of the Personal Data including establishing organizational policies for employees, agents and sub-contractors aimed at complying with the Data Processor's duties to safeguard the Personal Data in accordance with this Agreement, including but not limited to an AAAA "Authentication, Authorization, Accounting and Auditing" compliant computerized system;
- d) Implement backup processes as agreed between the Data Controller and Data Processor to procure the availability of the Personal Data at all times and ensure that the Data Controller will have access to such backup of the Personal Data as is reasonably required by the Data Controller;

- e) Ensure that any disclosure to an employee, agent or sub-contractor is subject to a binding legal obligation to comply with the obligations of the Data Processor under this Agreement including compliance with relevant technical and organizational measures for the confidentiality, privacy, integrity, availability, accuracy and security of the Personal Data. For the avoidance of doubt, any agreement with an employee, agent or sub-contractor shall not relieve the Data Processor of its obligation to comply fully with this Agreement, and the Data Processor shall remain fully responsible and liable for ensuring full compliance with this Agreement;
- f) Comply with any request from the Data Controller to amend, transfer or delete Personal Data; provide a copy of all or specified Personal Data held by it in a format and or a media reasonably specified by the Data Controller within reasonable timeframes as agreed between the Parties;
- g) Should the Data Processor receive any complaint, notice or communication which relates directly or indirectly to the processing of the Personal Data or to either Party's compliance with applicable law, immediately notify the Data Controller and provide the Data Controller with full co-operation and assistance in relation to any complaints, notices or communications;
- h) Promptly inform the Data Controller if any Personal Data is lost or destroyed or becomes damaged, corrupted or unusable and at the request of the Data Controller, restore such Personal Data at its own expense;
- i) In the event of the exercise by Data Subjects of any rights in relation to their Personal Data in accordance with Article 7 below, inform the Data Controller as soon as possible,
- j) Assist the Data Controller with all data subject information requests which may be received from any Data Subject in relation to any Personal Data;
- k) Not use the Personal Data of Data Subjects to contact, communicate or otherwise engage with the Data Subjects including transmission of any marketing or other commercial communications to the Data Subjects, except in accordance with the written consent of the Data Controller or to comply with a court order. For the avoidance of doubt, the Data Processor is not prohibited from contact, communication or engaging with the Data Subject in so far as this does not involve processing of Personal Data and the Data Processor procures that the promotion or offer of services is not in any manner associated to the Data Controller or the Data Controller's services;
- l) Notify the Data Controller of the country(s) in which the Personal Data will be processed wherever such country(s) is not the country of the Data Processor's registered office;

- m) Not process or transfer the Personal Data outside of the country of its registered office except with the express prior written consent of the Data Controller pursuant to a request in writing from the Data Processor to the Data Controller;
 - n) Permit and procure that its data processing facilities, procedures and documentation be submitted for scrutiny by the Data Controller or its authorized representatives, on request, in order to audit or otherwise ascertain compliance with the terms of this Agreement;
 - o) Advise the Data Controller of any significant change in the risk of unauthorized or unlawful processing or accidental loss, destruction or damage of Personal Data; and
 - p) Report in accordance with agreed reasonable timeframes to the Data Controller on the steps it has taken to ensure compliance with this Article 6 of the present Agreement.
- 6.2. If pursuant to any law or regulation affecting the Data Processor, Personal Data is sought by any governmental body, the Data Processor shall:
- (a) Promptly notify the Data Controller of this fact and consult with the Data Controller regarding the Data Processor's response to the demand or request by such governmental body;
 - (b) Inform such governmental body that such Personal Data is privileged due to the status of the Data Controller as a subsidiary organ of the United Nations, as a result of which it enjoys certain privileges and immunities as set forth in the Convention on the Privileges and Immunities of the United Nations (the "General Convention");
 - (c) Request such governmental body either to redirect the relevant request for disclosure directly to the Data Controller or to grant the Data Controller the opportunity to present its position regarding the privileged status of such Personal Data;
 - (d) cooperate with the Data Controller's reasonable requests in connection with efforts by the Data Controller to ensure that its privileges and immunities are upheld and, to the extent permissible by law, seek to contest or challenge the demand or request based on, inter alia, the Data Controller's status, including its privileges and immunities;
 - (e) Where the Data Processor is prohibited by applicable law or the governmental body from notifying the Data Controller of a governmental body's request for such Personal Data, notify the Data Controller promptly upon the lapse, termination, removal or modification of such prohibition;
 - (f) Provide the Data Controller with true, correct and complete copies of the governmental body's demands and requests, the Data Processor's responses thereto, and keep the Data Controller informed of all developments and communications with the governmental body. The obligations and restrictions set out in this Article 6 shall be effective during the term of this Agreement, including any extension thereof, and shall remain effective following any termination of this Agreement, unless

otherwise agreed between the Parties in writing

Article 7

Access of Data by Data Subjects

- 7.1. Every Data Subject who offers proof of identity shall have the right to know whether his/her personal data has been shared under this Agreement, and to obtain this data in intelligible form, without undue delay and free of charge This is subject to exceptions necessary to protect the privileges and immunities of the United Nations or of the Data Controller, the Data Controller's legitimate interests, national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others.
- 7.2. The Party that shared the data shall be consulted in order to determine whether any such exceptions apply to the personal data at issue, and any such determination made by that Party shall be binding.

Article 8

Compliance with National Legislation

- 8.1. The Data Processor warrants that it will:
 - a) Process the Personal Data in accordance with the terms and conditions set out in this Agreement and where the standards imposed by the data protection legislation regulating the Data Processor processing of the Personal Data are higher than those prescribed in this Agreement, then in accordance with such legislation;
 - b) Process the Personal Data in compliance with laws, enactments, regulations, orders, standards and other similar instruments applicable to the Data Processor; and in accordance with the terms and conditions of this Agreement;

Article 9

Indemnity

- 9.1. The Data Processor agrees to indemnify and keep indemnified and defend at its expense the Data Controller against all costs, claims, damages or expenses incurred by the Data Controller or for which the Data Controller may become liable due to any failure by the Data Processor or its employees, subcontractors or agents to comply with the obligations under this Agreement.

Article 10

Appointment of Sub-Contractors and Agents

- 10.1. The Data Processor may authorize a third party (sub-contractor or agent) to process Personal Data:
- a) subject to the terms of this Agreement;
 - b) subject to the Data Controller's prior written authorization, the validity of such consent shall be conditioned on the Data Processor supplying the Data Controller with full and accurate details of sub-contractors or agents;
 - c) the execution by such third party (sub-contractor or agent) of a written agreement with the Data Processor under which (i) such third party is bound to the same obligations of the Data Processor hereunder, (ii) UNHCR is expressly identified in such agreement as third-party beneficiary and such agreement provides that the obligations of such third party are made for the benefit of and are enforceable by the Data Processor in a binding arbitration procedure as described in the Contract and without waiver, express or implied, of any privileges and immunities of the United Nations, including its subsidiary organs, or of UNHCR (as a subsidiary organ of the United Nations), and
 - d) provided the relevant sub-contractor's or agent's contract terminates automatically on the termination of this Agreement for any reason.

Article 11

Settlement of disputes

- 11.1. Any dispute, controversy or claim between the Parties arising out of this Agreement shall be governed by the relevant provisions of Annex xxx to the Contract governing the settlement of disputes.

Article 12

Privileges and immunities

- 12.1. Nothing in or relating to this Agreement shall be deemed a waiver, express or implied, of any of the privileges and immunities of the United Nations, including its subsidiary organs or of the Data Controller (as a subsidiary organ of the United Nations).

Article 13

Entry into Force, Amendment and Termination

- 13.1. This Agreement shall enter into force on the date of its signature by both Parties and shall continue in force unless terminated under paragraphs 3 and 4 of this Article 13.
- 13.2. This Agreement may be modified at any time by mutual written consent.
- 13.3. This Agreement shall terminate automatically upon termination or expiry of the Contract.
- 13.4. The Data Controller shall be entitled to terminate this Agreement forthwith by notice in writing to the Data Processor if the Data Processor is in a material or persistent breach of this Agreement which, in the case of a breach capable of remedy, shall not have been remedied within 5 days from the date of receipt by the Data Processor of a notice from the Data Controller identifying the breach and requiring its remedy.
- 13.5. The obligations under Articles 6, 7 and 9 of this Agreement shall not cease with the termination of this Agreement.

Article 14

Return or Destruction of Personal Data

- 14.1. Upon the termination or expiration of this Agreement, the Data Processor shall draw up two categories of Data Subjects and treat their Personal Data in accordance with the following provisions.
- 14.2. Personal Data of all Data Subjects with no medical interventions:
 - a) The Data Processor shall destroy all the Personal Data of these Data Subjects in its possession or under its control, and in all forms (including but not limited to electronic, digital, physical form available online, offline or on backup, disaster recovery or archival systems) immediately upon termination or expiration of this Agreement.
 - b) The Data Processor shall instruct all its employees, agents and sub-contractors to facilitate and ensure the destruction of the Personal Data of these Data Subjects, including copies thereof, in accordance with paragraph 2.1 of Article 14.
 - c) xxxx shall submit to UNHCR a written confirmation signed by two authorized representatives that it has taken action in accordance with paragraph 2 (a) and (b) of this Article 14 within 1 (one) week of termination or expiration of this Agreement. Together with this confirmation, xxxx shall attach a digitally signed electronic file listing all Data Subjects under this category.

14.3. Personal Data of all Data Subjects with medical interventions:

- a) The Data Processor shall destroy all the Personal Data of these Data Subjects in its possession or under its control, and in all forms (including but not limited to electronic, digital, physical form available online, offline, or on backup, disaster recovery or archival systems) immediately upon termination or expiration of this Agreement unless this would lead to a conflict with applicable local auditing, financial, regulatory laws in effect.
- b) The Data Processor shall instruct all its employees, agents and sub-contractors to facilitate and ensure the destruction of the Personal Data of these Data Subjects, including copies thereof, in accordance with paragraph 3.1 of Article 14.
- c) xxxx shall submit to UNHCR a written confirmation signed by two authorized representatives that it has taken action in accordance with paragraph 3(a) and (b) of this Article 14 within 1 (one) week of termination or expiration of this Agreement
- d) Should data retention be required by law for certain Data Subjects of this category, xxxx shall immediately inform UNHCR and provide UNHCR with a digitally signed electronic file that shall contain the following information: Individual ID numbers or names of concerned Data Subjects, the data that will be retained, the data retention reason and/or basis and the data retention period. xxxx shall act in good faith and to the extent possible use data minimization techniques to reduce the retained Personal Data in its systems to a minimum in compliance with the applicable local laws on data retention.
- e) xxxx shall provide UNHCR with a written confirmation signed by two authorized representatives that all retained Personal Data has been destroyed within 1 (one) week of expiration of the applicable retention period.
- f) xxxx shall provide to UNHCR in good faith access to its systems and offices for 1 (one) month after the termination or expiration of this Agreement to enable UNHCR designated staff members to ascertain that the data destruction has occurred according to the above.

14.4 Notwithstanding the return or destruction of the Personal Data, the Data Processor shall continue to be bound by the confidentiality obligations under the Contract.

Article 15

Miscellaneous Provisions

15.1 Headings and titles used in this Agreement are for reference purposes only and shall not be deemed a part of this Agreement for any purpose whatsoever.

15.2 Unless the context otherwise clearly requires, (a) all references to the singular shall include the plural and vice versa and references to any gender shall include every gender; and

(b) any words following the word "include," includes," "including," "in particular" or any similar words or expressions shall be construed without limitation and accordingly shall not limit the meaning of the words preceding them or immediately following them.

15.3 This Agreement and everything herein contained shall inure to the benefit of, and be binding upon, the Parties and their respective successors and permitted assigns.

In witness whereof the undersigned, being duly appointed representatives of the Data Controller and the Data Processor, respectively, have on behalf of the parties signed this Agreement, in the English and *Arabic (if necessary)* language(s). For purposes of interpretation and in case of conflict, the English text shall prevail.

For the Data Processor xxxxx

For Data Controller UNHCR

XXXX, UNHCR representative, Lebanon