

ANNEX D
SUPPLEMENTARY AGREEMENT
CONCERNING THE PROTECTION OF PERSONAL DATA

between

THE OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR REFUGEES

("UNHCR")

and

[Contractor]

("Data Processor")

PREAMBLE

WHEREAS, UNHCR has contracted [Contractor] (hereinafter referred to as the "Data Processor") to render services which incorporate processing personal data on UNHCR's behalf as set out in the Service Contract (hereinafter the "Main Agreement") between UNHCR and the Data Processor;

WHEREAS, by virtue of its mandate and its Data Protection Framework including the General Policy on Personal Data Protection and Privacy¹, UNHCR has the obligation to ensure that the privacy and Personal Data of individuals are protected in the processing of such data, whether independently or through the engagement of third parties acting on UNHCR's behalf;

NOW, THEREFORE, UNHCR and the Data Processor (the "Parties") hereby agree as follows:

Section 1. Certain Definitions.

1.1. In this Supplementary Agreement, the following terms have the following meanings given to them, unless the context otherwise requires:

- (a) "Personal Data" means any information relating to an identified or identifiable individual ("Data Subject") processed by the Data Processor on behalf of UNHCR under this Agreement and the Main Agreement.
- (b) "Processing" means any operation, or set of operations, automated or not, which is performed on Personal Data, including but not limited to the collection, recording,

¹ UN High Commissioner for Refugees (UNHCR), General Policy on Personal Data Protection and Privacy, 20 December 2022, <https://www.refworld.org/policy/strategy/unhcr/2022/en/124207>.

organization, structuring, storage, adaption or alteration, retrieval, consultation, use, transfer, dissemination or otherwise making available, correction, restriction or destruction.

- (c) “Services” means the specific activities for which UNHCR has engaged Data Processor as set out in the Main Agreement.
- (d) “Data Security Breach” means a breach of data security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, UNHCR Data including as concerns Personal Data transferred, stored or otherwise processed.
- (e) “UNHCR Personnel” means UNHCR staff members and affiliate workforce. UNHCR’s affiliate workforce are individuals who have a working relationship with UNHCR, including United Nations Volunteers (UNVs), individual consultants, individual contractors (including contractors under arrangements with the United Nations Office for Project Services (UNOPS) or another affiliate Data Processor organization), fellows and employees.
- (f) “UNHCR Data” means any and all information, whether in oral or written (including electronic) form, created by or in any way originating with UNHCR and/or its personnel, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with UNHCR and/or its personnel, shared with the Data Processor when providing the Services, and specifically includes, without limitation, any and all UNHCR data including Personal Data and anonymized data processed by the Data Processor on behalf of UNHCR. For the avoidance of doubt, UNHCR Data shall include: (i) all data shared with Contractor in connection with the Services as defined in Article 2.2 above; (ii) all data collected (including Personal Data of UNHCR personnel) by the Contractor in providing the Services (iii) all data developed by, or in connection with, the Services.

- 1.2. Unless the context otherwise requires, capitalized terms used but not otherwise defined in this Supplementary Agreement shall have the meanings given to them in the Main Agreement.

Section 2. Personal Data Processing

- 2.1. This Supplementary Agreement pertains to the protection of UNHCR Data including Personal Data accessed, collected or otherwise received and processed by the Data Processor on UNHCR’s behalf in the course of rendering the Services. The Data Processor shall process the Personal Data strictly for the specific purposes and other documented instructions of UNHCR and for no other purpose or in any other manner except with the express prior written authorization of UNHCR.
- 2.2. The Data Processor shall process the Personal Data in accordance with the terms and conditions set out in this Supplementary Agreement and where the standards imposed by the data protection legislation regulating the processing of the Personal Data are higher than those prescribed in this Supplementary Agreement, then in accordance with such legislation.
- 2.3. The Data Processor shall not process any Personal Data 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 authorization of UNHCR or to comply with a court order subject to its obligations under Section 4.6 below.

Section 3. Data Processor’s Obligations

- 3.1. Confidentiality. In accordance with Article 13 of UNHCR General Conditions of Contract for the Provision of Services (Annex A to the Main Agreement), the Data Processor shall regard Personal Data as confidential data and not disclose such data without the prior written authorization of UNHCR to any person other than to its personnel, agents or sub-contractors to whom disclosure is necessary for the performance of the Services, except (subject to Section 3.8 below) as may be required by any law or regulation affecting the Data Processor.
- 3.2. Security of Personal Data. The Data Processor shall implement appropriate technical and organisational measures to safeguard the Personal Data from unauthorised 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 unauthorised or unlawful processing or accidental loss, destruction or damage and to the nature of the Personal Data to be protected. Without limiting the foregoing, the Data Processor shall:
- (a) implement technical and organisational measures to procure the confidentiality, privacy, integrity, availability, accuracy and security of the Personal Data including to ensure that any disclosure to an employee, agent or sub processor is subject to a binding legal obligation to comply with the obligations of the Data Processor under this Supplementary Agreement including compliance with relevant technical and organisational measures for the confidentiality, privacy, integrity, availability, accuracy and security of the Personal Data including, without limitation, anti-virus and anti-malware protections, intrusion detection and reporting methods (alerts are captured and analysed in real time). For the avoidance of doubt, any agreement, contract or other arrangement with an employee, agent or sub-Processor shall not relieve the Data Processor of its obligation to comply fully with this Supplementary Agreement, and the Data Processor shall remain fully responsible and liable for ensuring full compliance with this Supplementary Agreement;
 - (b) ensure that the Personal Data are stored in a secure (encrypted) digital and physical environment;
 - (c) ensure that all UNHCR data sharing is executed by secure (end-to-end encrypted) means, in particular ensure encryption of all devices including mobile devices, storage devices files and databases containing Personal Data and encrypt all communications between UNHCR and the Data Processor, between Data Processor and all third parties (including its Sub-Processors);
 - (d) implement technical measures including (i) restricting access to data to authorized personnel and devices only, (ii) the use of multi-factor authentication where possible, and passwords to prevent unauthorized access to data and (iii) backing-up data in case of loss or damage;
 - (e) implement organizational measures including (i) securing premises where hard-copy files or computers are stored, (ii) safely disposing of any obsolete hard copy files and (iii) ensuring that portable devices are always kept in a secure location when not in use.
 - (f) implement backup processes and reliable storage media as agreed between UNHCR and the Data Processor to always procure the availability of the Data and ensure that UNHCR will have access to such backup of the Data as is reasonably required by UNHCR. All backup copies of Data shall be retained for a minimum of 12 months following their respective creation.

- (g) comply with any request from UNHCR 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 UNHCR within reasonable timeframes as agreed between the Parties;
- (h) At the written election of UNHCR, the Contractor shall either securely destroy or transmit to UNHCR, or to a third party designated in writing by UNHCR, any backup copies of the Data.
- (i) The Contractor shall provide UNHCR a written certificate indicating the nature or type of Data disposed of, the date of such disposal, and the method of disposal.
- (j) inform UNHCR of the location of its processing the Personal Data and immediately notify UNHCR of any changes. The Data Processor shall process the Personal Data only within member State(s) that have recognized the privileges and immunities of the United Nations pursuant to the General Convention or any other relevant international or national legal instrument. Under no circumstance shall any Personal Data of refugees or asylum seekers be transferred to their country of origin.

3.3. Information Security In addition to the requirements set forth in the Article 3.2, the Data Processor shall:

- (a) comply with UNHCR's instructions on IT security, include the security controls and countermeasures considered required according to UNHCR information security baselines, and when requested by UNHCR permit information security reviews and/or audits in accordance with Article 3.5 below;
- (b) implement information security measures which shall be no less protective than those used by the Data Processor to protect its own confidential information, and in no event less than reasonable in view of the nature and type of data involved. As such, the Contractor shall implement and maintain industry-standard security measures (as evidenced, for example, by an ISO 27001 certificate and/or a SOC 2 type 2 report) to protect UNHCR Data from unauthorized access, disclosure, alteration, and destruction;
- (c) ensure that Data is logically segregated from other customer's data to the fullest extent possible;
- (d) provide the Data Controller at the latest upon the signature of the Agreement with a description of such information security measures, which shall include at least:
 - i. ensuring the ongoing confidentiality, integrity, availability of processing systems and services;
 - ii. protection of all UNHCR Data against deterioration or degradation of its quality and authenticity;
 - iii. platform has an Intrusion Detection System or Intrusion Prevention System (IDS/IPS) running and its alerts are analysed in real time and is protected by a network firewall or network security group, and the firewall/NSG rules are documented and actively managed by the managing organization;

- iv. platform is behind a Web Application Firewall (WAF), running in blocking mode (whereby traffic detected as suspicious is automatically blocked);
- v. Mobile application interface meet OWASP mobile app standards.
- vi. a process for regularly testing, assessing and evaluating the effectiveness of the information security measures implemented;
- vii. fast restoration of the availability of, and access to, UNHCR Data in the event of Personal Data Breach or other data security incident; and
- viii. regular verification, evaluation and assessment of the effectiveness of information security measures,
- ix. implementing and maintaining industry-standard security measures (comparable to those required by an ISO 27001 certificate and/or a SOC 2 type 2 report) to protect UNHCR Data from unauthorized access, disclosure, alteration, and destruction;
- x. ensuring to patch, version and maintain all software used to deliver the Services to highest standards (always version N or N-1) including an emergency patch process for critical vulnerabilities;
- xi. Coordinating with UNHCR in ensuring that all UNHCR Data is backed up on a daily basis and paper-based information is duly secured in protected UNHCR premises;
- xii. maintaining a data governance framework according to the risks of the information accessed;

3.4. Audit. The Data Processor shall permit and procure that its data processing protocols (in connection to its access to UNHCR systems), procedures and documentation be submitted for scrutiny by UNHCR or its authorised representatives, on request, including the provision of a copy of its most recent SOC 2 Type 2 report, in order to audit or otherwise ascertain compliance with the terms of this Agreement. Following any actual or reasonably suspected unauthorized disclosure of Personal Data shared by UNHCR with the Data Processor, in accordance with Article 23 (Audits and Investigations) of UNHCR General Conditions of Contract for the Provision of Services (Annex A to the Main Agreement), UNHCR shall have the right to conduct, pursuant to appropriate confidentiality and technical restrictions, an on-site audit of the Data Processor's or its affiliates' systems, policies, and procedures relevant to the security and integrity of UNHCR Data.

3.5. Requests or complaints concerning compliance with law. 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 UNHCR and provide UNHCR with full co-operation and assistance in relation to any complaints, relating notices or communications.

3.6. Notification of Data Security Breach. The Data Processor shall,

- (a) promptly within 48 hours inform UNHCR upon becoming aware of any actual or potential Personal Data Breach and shall use its best efforts to follow UNHCR's instructions to take mitigating measures.
- (b) advise UNHCR of any significant change in the risk of unauthorised or unlawful processing or Personal Data Breach.

3.7. Responsibilities relating to Data Subjects. The Data Processor shall observe the following responsibilities relating to Data Subjects:

- (a) In the event of a request by a Data Subject to exercise their rights to information, access, correction, deletion and objection in relation to their Personal Data, the Data Processor shall inform UNHCR as soon as possible and follow UNHCR's reasonable instructions;
- (b) The Data Processor shall assist UNHCR with all data subject requests or complaints which may be received from a Data Subject in relation to their Personal Data.

3.8. Non-disclosure to Governmental bodies. The Data Processor recognizes that any UNHCR Data, including without limitation Personal Data, to be processed by the Data Processor pursuant to this Supplementary Agreement is part of UNHCR assets and is subject to the privileges and immunities accorded to the United Nations, including UNHCR, and as such (i) shall be deemed part of UNHCR's archives which are inviolable wherever located and by whomever held and may be disclosed, (ii) shall be immune from search, requisition, confiscation, and any form of interference by any party, whether by executive, administrative, judicial or legislative action, unless such immunity is expressly waived in writing by UNHCR. 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 UNHCR of this fact and consult with UNHCR 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 UNHCR 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 UNHCR or to grant UNHCR the opportunity to present its position regarding the privileged status of such Personal Data;
- (d) cooperate with UNHCR's reasonable requests in connection with efforts by UNHCR 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, UNHCR's status, including its privileges and immunities;
- (e) where the Data Processor is prohibited by applicable law or the governmental body from notifying UNHCR of a governmental body's request for such Personal Data, notify UNHCR promptly upon the lapse, termination, removal or modification of such prohibition;

- (f) provide UNHCR with true, correct and complete copies of the governmental body's demands and requests, the Data Processor's responses thereto, and keep UNHCR informed of all developments and communications with the governmental body.
- 3.9. Sub-processors and Agents. The Data Processor may authorise a third-party sub-processor or agent to process the Personal Data, so long as such authorisation does not otherwise violate the Data Processor's obligations under this Supplementary Agreement and subject to the following conditions:
- (a) UNHCR's prior expressed written authorization, the validity of such authorization being conditioned on the Data Processor supplying UNHCR with full and accurate details of such third party sub-processor or agent at least 30 days in advance; and
 - (b) the execution by such third party Data Processor or agent of a written agreement with the Data Processor under which (i) such third party Data Processor or agent 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 Data Processor or agent are made for the benefit of and are enforceable by UNHCR in a binding arbitration procedure as described in the Main Agreement and without waiver, express or implied, any of the privileges and immunities of the United Nations, including its subsidiary organs, or of UNHCR (as a subsidiary organ of the United Nations) and (iii) the agreement terminates automatically on the expiry or termination, for any reason, of this Supplementary Agreement.
 - (c) UNHCR is provided an original counterpart of the agreement referred to in Section **Error! Reference source not found.**, signed by all parties thereto;
 - (d) The Data Processor shall promptly notify UNHCR of any breach of a third-party's obligations under an agreement referred to in Section **Error! Reference source not found.** and shall use reasonable efforts to enforce the obligations of the third party thereunder. The Data Processor shall provide reasonable assistance to UNHCR to support enforcement by UNHCR, as third party beneficiary, of the obligations of the third party under such agreement.

Section 4. Representations and Warranties

- 4.1. *Service Warranty*. The Contractor represents and warrants to UNHCR that the Services as described in Annex B shall :
- (a) conform to the specifications agreed with UNHCR;
 - (b) be performed, function and produce results substantially in accordance with such specifications;
 - (c) be free and clear of any and all liens, claims, encumbrances or demands of third parties (collectively, the "Services Warranty").
- 4.2. In the event of a breach of the Service Warranty, UNHCR shall provide the Contractor prompt notice thereof, and the Contractor, at its sole cost and expense, shall promptly correct or replace the portion of the Services implicated in such breach. If the Contractor fails to cure any breach of the Services Warranty by a reasonable date prescribed by UNHCR in its notice, UNHCR may,

in its sole discretion, either extend the time for the Contractor to cure the breach or terminate this Contract and receive a full refund of all amounts paid to the Contractor under this Contract.

- 4.3. *Disabling Code Warranty.* The Contractor represents and warrants to UNHCR that the Services as described in Annex B shall not contain, any virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design, or other malicious, illicit or similar unrequested code, including surveillance software or routines which may, or is designed to, permit access by any person, or on its own, to erase, or otherwise harm or modify any UNHCR Data or any system, server, facility or other infrastructure of UNHCR (collectively, a "Disabling Code").
- 4.4. All Contractor's personnel, subcontractors and agents directly involved in the delivery of the Services shall be trained in UNHCR's security requirements in mandatory UNHCR training courses or approved materially equivalent training in secure coding practices.
- 4.5. Except with the prior written authorization of UNHCR, the Contractor's personnel, subcontractors or agents shall not: (a) introduce or install any software, tools or utilities whatsoever on UNHCR computer equipment; (b) connect their own computers to the UNHCR computer network; or (c) introduce any magnetic or optical information technology storage media into UNHCR computer equipment, or download any program or file whatsoever from the Internet into UNHCR computer equipment, unless such actions are pursuant to routine UNHCR information technology management and maintenance procedures, using files or media from a known and approved source such as the official providers of application, database or utility software.
- 4.6. If Contractor's personnel, subcontractors or agents will use their own equipment (personal, or provided by the Contractor) to access UNHCR information systems, such equipment shall meet a minimum baseline, including current operating system, current OS and application patches, full-disk encryption, current antivirus and/or EDR tool. The equipment should be kept physically secure at all times, and should not be shared with others.
- 4.7. Any software security defects caused by the Contractor's staff personnel, subcontractors or agents shall be remedied by the Contractor without any additional costs for UNHCR.

Section 5. Data Protection Impact Assessment

- 5.1. Upon UNHCR's request, the Data Processor shall provide UNHCR with reasonable cooperation and assistance needed to carry out a data protection impact assessment related to UNHCR's use of the services.
- 5.2. The Data Processor shall implement at any time, any recommendation, arising out of UNHCR's data protection impact assessments.

Section 6. Liability and Indemnity

- 6.1. Without prejudice to the Contractor's liability pursuant to Article 8.1 of the UNHCR General Conditions of Contract for the Provision of Services (Annex A), the Contractor shall pay UNHCR promptly for all loss incurred due to a breach of its obligations relating to data security and processing of personal data.
- 6.2. The Contractor agrees to indemnify and keep indemnified and defend at its expense UNHCR against all costs, claims, damages or expenses incurred by UNHCR or for which UNHCR may

become liable due to any failure by the Contractor's personnel, subcontractors or agents to comply with the obligations under this Supplementary Agreement.

Section 7. Termination.

- 7.1. This Supplementary Agreement shall terminate automatically upon termination or expiration of the Main Agreement.
- 7.2. The obligations and restrictions in Section 4 of this Supplementary Agreement shall be effective during the term of this Supplementary Agreement, including any extension thereof, and shall remain effective following any termination of this Supplementary Agreement, unless otherwise agreed between the Parties in writing.

Section 8. Return and Deletion of Personal Data.

- 8.1. After expiration or termination of this Supplementary Agreement, the Data Processor shall delete Personal Data subject to the relevant provisions set out in Annex C.
- 8.2. Such deletion shall be evidenced by a written attestation issued to UNHCR and signed by two authorized representatives of the Data Processor.
- 8.3. The Data Processor shall give written notice to UNHCR of any Personal Data it is legally obliged to retain under applicable law or as per internal auditing requirements for a certain time period following the expiration of this Agreement, the Data Processor shall notify UNHCR of this in writing, shall no longer actively process the data for any other purpose, and shall destroy the data immediately after this time period has expired. The Data Processor shall promptly destroy such retained Personal Data as soon as permitted under applicable law, and its obligations under this Supplementary Agreement shall survive until such retained Personal Data is destroyed in accordance with this Section 8.
- 8.4. Notwithstanding the deletion of the Personal Data, the Data Processor shall continue to be bound by the confidentiality obligations under the Main Agreement.

Section 9. Dispute Resolution.

Any dispute, controversy or claim between the parties arising out of this Supplementary Agreement shall be governed by the relevant provisions of the Main Agreement governing the settlement of disputes.

Section 10. Privileges and Immunities.

Nothing in or relating to this Supplementary 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 UNHCR (as a subsidiary organ of the United Nations).

Section 11. Miscellaneous Provisions.

- 11.1. 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.

11.2. 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.

11.3. 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 Parties have caused their duly authorized representatives to append their signatures below as of the date first stated above.

For and on behalf of:
**THE OFFICE OF THE UNITED NATIONS
HIGH COMMISSIONER FOR REFUGEES**

For and on behalf of:
[Data Processor]

Signature

Name:

Title:

Date:

Place:

Signature

Name:

Title:

Date:

Place: