ADDENDUM ON DATA SHARING

TO

THE JANUARY 2011 MEMORANDUM OF UNDERSTANDING

BETWEEN

THE OFFICE OF THE UNITED NATIONS
HIGH COMMISSIONER FOR REFUGEES (UNHCR)

AND

THE WORLD FOOD PROGRAMME (WFP)

September 2018

Table of Contents

Annexes

SECTION 1. INTRODUCTION

1.1 The January 2011 Memorandum of Understanding (hereafter the "**Global MoU**") between the Office of the United Nations High Commissioner for Refugees (UNHCR) and the World Food Programme (WFP) establishes the framework for their partnership and collaboration.

1.2 According to the Section 3.37 on Information Management of the Global MoU, UNHCR and WFP have agreed to "collaborate on defining standards and developing a mechanism for exchanging information on beneficiaries, including geographic information and associated technologies. All data exchange will be done in accordance with international and United Nations standards for data protection and privacy, in full recognition of the sensitive nature of beneficiary data [...]."

1.3 Furthermore, in line with the Addendum on Cash Assistance to Refugees to the Global MoU of 15 May 2017, "UNHCR and WFP recognize the importance of jointly analysing and sharing relevant data to ensure that cash and other assistance is effective and avoids duplication." This Addendum serves to provide a framework for this collaboration.

1.4 The past decade has seen dramatic change in the humanitarian landscape with an increase in the number of protracted crises, and the subsequent drive towards more integrated interventions that address the root causes and better support long term, sustainable solutions and resilience. By partnering on data sharing, WFP and UNHCR endeavour to bring about greater efficiency and efficacy in our assistance to those furthest behind, in line with global commitments and realization of the Sustainable Development Goals (SDGs).

1.5 This Addendum is grounded in the mutual objective of ensuring that the well-being of all those served by the Agencies is central to efforts, in particular that their protection, safety and dignity is ensured including through the protection and responsible use of data.

1.6 Building the organizational collaboration and communication between UNHCR and WFP, this Addendum seeks to facilitate country level dialogue and leadership in our collective work to meet the basic needs of all Persons of Concern (PoCs), acknowledging that this is one component of our overall continued partnership.[1] With the premise of this Addendum being the collaborative, timely sharing of data at country level working towards inter-agency inter-operability, it also provides an important platform for joint assessment, analysis, planning, identity management, programming and monitoring for better service delivery.

1.7 The collective accountability of UNHCR and WFP to affected populations will be further enhanced through the implementation of this Addendum which seeks to integrate and align the knowledge and expertise to secure the best possible outcomes for those UNHCR and WFP serve.

1.8 UNHCR and WFP are committed to ensuring the protection of personal data through respective documents issued since the conclusion of the Global MoU: the UNHCR Policy on the Protection of Personal Data of Persons of Concern (2015) and the WFP Guide to Personal Data Protection and Privacy (2017) (the "Data Protection Framework"). Both documents confirm the Agencies' commitments to respect internationally recognized data protection principles, particularly that of purpose specificity and proportionality. These documents form the basis for the sharing of Personal Data under this Addendum.

1.9 Against this background and in accordance with their respective information disclosure policies, the Agencies agree to a collaborative and efficient approach to data sharing, particularly in support of country offices.

---

[1] Memorandum of Understanding between the Office of the United Nations High Commissioner for Refugees (UNHCR) and the World Food Programme (WFP), January 2011; Addendum on Cash Assistance to the Refugees to the January Memorandum of Understanding between the United Nations High Commissioner for Refugees (UNHCR) and the World Food Programme (WFP); Joint Strategy for Enhancing Self-Reliance in Protracted Refugee Situations; and the UNHCR –WFP Joint Targeting Principles 2017.

1.10 The principal elements of this Addendum are commitments by WFP and UNHCR to share specific Personal Data, Non-Personal Data and Information for specific purposes as agreed in Annex 1 of this Addendum. Request for Personal Data, Non-Personal Data and Information should follow the processes outlined in Sections 4 and 5 of this Addendum utilising respective Request Forms (Annex 2 and Annex 3).

1.11 For the purposes of this Addendum, Persons of Concern are refugees, asylum-seekers, returned refugees (returnees), stateless persons, internally displaced persons and host populations.

SECTION 2. DEFINITIONS

The following definitions apply for this Addendum:

"Agency" or **"Agencies"** refers to either WFP or UNHCR, or both, as the context requires.

"Anonymized Data" means data from a set of Personal Data from which all identifying elements have been eliminated with the effect that no element is left which could, by means reasonably likely to be used, serve to re-identify the Data Subject.

"Data Protection Framework" means each Agency's respective policies and guidelines with regard to the protection of personal data of Persons of Concern, including the documents referred to in Section 1.8.

"Data Subject" means an individual whose Personal Data is subject to processing.

"Information" means any non-personally identifiable information relating to Persons of Concern in text or non-machine readable format (such as reports or other operational, transactional or other information), but in any case excluding e-mails.

"Joint Data Sharing Support Group" is comprised of staff from both Agencies and aims to support the implementation of this Addendum as outlined in Section 8.

"Metadata" means structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource (footnote: "Understanding Metadata," National Information Standards Organization (NISO) http://www.niso.org, ISBN: 1-880124-62-9, 2004). The Metadata provided in the context of this Addendum is set out in Annex 1. Metadata represents Non-Personal Data and if there is any personally identifiable metadata (e.g. data collector name) this should be eliminated from such set prior to sharing. In exceptionally protection sensitive contexts, some non-personal metadata may need to be removed to avoid doing harm. Metadata requirements may vary according to the context and the systems they need to pass between, but in this Addendum minimum required metadata fields are listed in Annex 1.

"Non-Personal Data" means any single data items, data sets (collection of cleaned and processed data) and data results (output of analyzed data) that are not Personal Data.

"Personal Data" means any information related to an identified or identifiable Data Subject. Personal Data includes "Biographic Data" for example, a name, sex, date and place of birth, an identification number, and also includes "**Biometric Data**" which includes a facial photograph, fingerprint, and or iris biometric images, and/or biometric templates derived from the aforementioned biometric images.

"Personal Data Breach" means a breach of data security leading to the accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data shared, stored or otherwise processed.

"Persons of Concern" for the purposes of this Addendum, include refugees, asylum-seekers, returned refugees (returnees), stateless persons, internally displaced persons and host populations (as per Section 1.11).

"Request Form" means:

(i) the request for the sharing of Non-Personal Data and Information in the form set out in Annex 2; and
(ii) the request for the sharing of Personal Data in the form set out in Annex 3.

SECTION 3. OBJECTIVE OF THE ADDENDUM

3.1 The objective of this Addendum is to set out a global framework with the terms, conditions and processes for Data sharing, including the sharing of Personal Data, Non-Personal Data and Information, between the Agencies.

3.2 By means of this Addendum, the Agencies intend to reach the following specific objectives:

(i) to ensure timely provision of relevant Data for improved protection, programmatic coherence and efficiency;
(ii) to ensure security of Data;
(iii) encourage interoperable systems and joint platforms;
(iv) to enhance accountability mechanisms vis-a-vis Persons of Concern; and
(v) where possible, to reduce duplicate data-collection and overlapping of other data-related activities between the Agencies.

SECTION 4. SHARING OF NON-PERSONAL DATA AND INFORMATION

4.1 Process for sharing of Non-Personal Data and Information contained in Annex 1

4.1.1 The Agencies agree to share Non-Personal Data and Information identified in Column C and qualified as Non-Personal Data or Information in Column E of Annex 1 in accordance with this Section 4.1.

4.1.2 The Agencies will request Non-Personal Data and Information identified in Annex 1 by means of Request Form (Annex 2) or by means of a simple, informal communication (including by e-mail) with the content of such Request Form.

4.1.3 A request to share Non-Personal Data and Information identified in Annex 1 may be rejected in the following situations:

(i) it would otherwise breach a contract with a third party;
(ii) the requested Agency does not have the requested Non-Personal Data or Information; and/or
(iii) if the sharing, publicizing or further processing of Non-Personal Data or Anonymized Data is likely to pose risks to Persons of Concern, humanitarian actors or other stakeholders.

Each Agency will endeavor to ensure that no reason to reject a request for the sharing of Non-Personal Data or Information arises. To the extent possible, the requested Non-Personal Data and Information will be made available in an up-to-date and clean form.

4.1.4 The requested Agency will provide a written response within one week from the date of this request indicating whether and when the data will be shared.

4.1.5 Any disagreement or other dispute arising out of or relating to the sharing pursuant to this section may be escalated for resolution in accordance with the Escalation Process set out in Section 7.

4.2 Process for sharing of Non-Personal Data and Information not contained in Annex 1

The expectations in relation to the sharing of Non-Personal Data and Information set out in this Addendum will only apply to that set out in Annex 1. Any Non-Personal Data and Information not identified in Annex 1 may be shared using the same request process, following the Escalation Process set out in Section 7. Each Agency will endeavor to share such Non-Personal Data and Information within the spirit and objectives of this Addendum.

4.3 Confidentiality

Non-Personal Data or non-publicly available Information shared may not be shared or otherwise disclosed to any third party unless otherwise agreed. Where the receiving Agency publishes reports or studies based on the Non-Personal Data or Information received from the sharing Agency, the source of the data (namely, the sharing Agency) will be acknowledged.

SECTION 5. SHARING OF PERSONAL DATA

5.1 General Commitments relating to the Processing of Personal Data

5.1.1 Similarly High Levels of Personal Data Protection. The Agencies acknowledge that their respective Data Protection Frameworks contain, and Agencies are therefore subject to similarly high levels of Personal Data protection, corresponding protection mechanisms as well as corresponding principles relating to the processing of Personal Data and therefore trust that the relevant other Agency is complying with its Data Protection Framework.

5.1.2 Principles of Personal Data Protection. The Agencies recognize the following core principles set out in the respective Data Protection Frameworks and agree to adhere to such principles when processing and sharing Personal Data of Persons of Concern in accordance with this Addendum:

(i) **Legitimate and fair collection and processing:** Processing of Personal Data may only be carried out on a legitimate basis and in a fair and transparent manner. The Agencies may only process Personal Data for the general purpose of carrying out their respective mandates and based on one or more of the following legitimate bases:

   a. with the informed consent of the Data Subject; or
   b. as a last resort, in the vital or best interest of the Data Subject.

(ii) **Purpose specification:** Personal Data will be collected for one or more specific and legitimate purpose(s) and should not be processed in any way incompatible with this/those purpose(s).

(iii) **Necessity and proportionality:** The processing of Personal Data should be adequate, relevant and not excessive to the purpose(s) for which it is being processed.

(iv) **Respect for the Data Subject's rights:** Data Subjects have rights in relation to information, access, correction and, deletion of their Personal Data and objection to its processing during all stages of such processing.

(v) **Security:** In order to ensure the confidentiality and integrity of Personal Data, appropriate technical and organizational data security measures need to be put in place.

5.2 Process for Sharing of Personal Data

5.2.1 Process for sharing of Personal Data contained in Annex 1

(i) The Agencies agree to share Personal Data relating to Persons of Concern as identified in column C and qualified as Personal Data in column E of Annex 1 in accordance with this Section 5.2.1. For the avoidance of doubt, a Country Office is permitted to request Personal Data elements identified in Annex 1 only where considered necessary and proportionate to the purpose specified.

(ii) The Agencies will request Personal Data identified in Annex 1 through a formal communication in the form of the Request Form (Annex 3). The request will be signed by an authorized representative of the requesting Agency.
(iii) The requested Agency will provide a written response within one week from the date of the request indicating whether and when the data will be shared.
(iv) To the extent possible, the requested Personal Data will be made available in a clean and up-to-date form.
(v) Further to 5.2.1(i), each of the requested Personal Data elements will be shared unless a valid reason would justify the rejection of such Personal Data element or all of the request. It is necessary to demonstrate that the non-sharing of some or all of the requested Personal Data would pose less risk for the Persons of Concern than the benefit of sharing such Personal Data. When making this evaluation, the requested Agency will take into account protection considerations, data protection and the need to provide assistance and protection response in a timely manner.
(vi) Any disagreement or other dispute arising out of or relating to the sharing of the Personal Data pursuant to this section may be escalated for resolution in accordance with the Escalation Process set out in Section 7.

5.2.2 Process for sharing of Personal Data not identified in Annex 1

(i) The expectations in relation to the sharing of Personal Data set out in this Addendum apply only to Personal Data identified in Annex 1. In addition, the Agencies may share Personal Data relating to Persons of Concern, which is not identified in Annex 1. Each Agency will endeavour to share such Personal Data within the spirit and principles set out in the introduction and the objectives of this Addendum (Section 1 and 3).
(ii) Such data may be requested through the form attached as Annex 3 and signed by an authorized representative of the requesting Agency.
(iii) The requested Agency will assess in good faith whether it can share the requested Data (e.g. if in accordance with its Data Protection Framework, information disclosure policies or otherwise in line with the requesting Agency's rules and regulations).
(iv) If it intends to do so, the Request Form will be countersigned by an authorized representative indicating whether and when the data will be shared. The Agencies commit to respond to such requests in a timely manner in the spirit of this Addendum.
(v) The Agencies commit to seek to resolve any disagreement or other dispute arising out of or relating to the sharing of the Personal Data pursuant to this section at country level, following which such disagreement may be referred for consultation and recommendation to the relevant regional bureau or to the Joint Data Sharing Support Group.
(vi) Any disagreement or other dispute arising out of or relating to the sharing of the Personal Data pursuant to this section may be escalated for resolution in accordance with the Escalation Process set out in Section 7.

5.2.3 Means of sharing Personal Data

(i) Any sharing of Personal Data will occur in a secure format, including but not limited to machine-readable electronic transfer or accessed via an online platform or through an Application Programming Interface (API).
(ii) Data may be made available by transmitting a copy of the Data Set ("Data Transfer") or by granting access to a Data Set held with an Agency ("Data Access"). In the latter case the requesting Agency does not obtain a copy of, but accesses the Data Set of the other Agency, for example through tools and systems provided by the data holding Agency (such as authentication services for Biometric Data) or by tools provided by the requesting Agency to securely access the data of the other Agency (e.g. through an API). Both Agencies will endeavor to advance technical developments and operational change management as required in order to facilitate Data Access or Data Transfer.

(iii) Sharing of Personal Data (Other than Biometric Data)

a) The Agencies aim to further establish interoperable systems and technologies which would allow Data Access to be sufficient in facilitating enhanced protection and assistance delivery. However, they acknowledge that this approach may not currently reflect operational realities. Therefore, in order to provide assistance in the current operational contexts, Data sharing of Non-Biometric Personal Data will occur through Data Transfer, unless as designed in paragraph (b) below.
b) Where Data sharing of Non-Biometric Personal Data through Data Access is technically and programmatically feasible, and can be implemented in compliance with each Agency's internal and external control frameworks, the Agencies will endeavor to establish Data Access as the means for sharing Personal Data.

(iv) Sharing of sensitive Biometric Data

The Agencies acknowledge that sensitive Biometric Data (such as iris scan and fingerprints, hereafter "Sensitive Data") require special protection. Copies of such Sensitive Biometric Data will therefore only be transferred when:

a) Data Access to Sensitive Biometric Data is not reasonably possible, including (but without limitation) when assistance is being implemented offline; and/or
b) each Agency's mandate (including the objective of this Addendum) cannot be reasonably achieved with Data Access only.

In all other scenarios covered by this Addendum, with respect to such Biometric Data, the Agencies agree to:

a) provide each other access to the relevant other Agency's Sensitive Biometric data through automated services for purposes of identity authentication and validation;
b) conduct joint biometric deduplication activities;
c) provide suitable copies of Sensitive Biometric Data to allow configuration of delivery mechanisms necessary for assistance programming and delivery, with each Agency's assurance that no copy is retained; and
d) identify common standards for biometric templates for the above.

5.3 Accountabilities with respect to shared Personal Data

5.3.1 General accountability with respect to Data Subject rights

(i) Each Agency will with respect to its own data sets, prior and after sharing, be accountable vis-à-vis the Data Subject, respecting the following Data Subject rights. Additionally, the receiving Agency will become accountable vis-à-vis the Data Subjects whose Personal Data was shared with it for the following Data Subject rights:

a) the right to receive information about data processing by the respective Agency;
b) the right to object to the processing of their Personal Data by the respective Agency;
c) the right to request access to data held by the respective Agency to whom it has been transferred;
d) the right to request the correction and/or deletion of that data held by the respective Agency; and
e) the right to submit complaints / feed-back to the respective Agency regarding the use of their data by such Agency.

(ii) The Agencies will endeavour to cooperate with respect to the fulfilment of such Data Subject rights. This includes the development and implementation of processes for such purpose. For example, Agencies will endeavour to establish joint country-level complaints and feedback handling mechanism that provides for complaints, concerns or requests on the part of Data Subjects to be addressed in a timely manner.

5.3.2 Accuracy of Personal Data Sets

(i) Unless otherwise agreed, the sharing Agency will be responsible in accordance with its Data Protection Framework for the update, maintenance and resolution of discrepancies relating to shared Personal Data.

(ii) The Agencies will cooperate with respect to the accuracy of the shared Personal Data. This includes developing and implementing processes to allow the Agencies to perform their accountabilities set forth in this Section.

(iii) In particular, should inconsistencies or errors in the data be identified and/or requests for changes to Personal Data be received by the recipient Agency, it will inform the sharing Agency so that it may take appropriate actions in accordance with its Data Protection Framework. The sharing Agency will inform the receiving Agency about any changes in the shared data set.

(iv) The performance of these accountabilities will be conducted in support of Data Subject rights referred to in Section 5.3.1.

5.3.3 Use, Processing and Onward Sharing of Shared Personal Data

(i) The receiving Agency agrees that it will use Personal Data shared under this Addendum in a manner compatible with the purposes for which it was shared. Where consent of the Data Subject has been obtained for the use of their Personal Data for other purposes, the receiving Agency may use the Personal Data accordingly.

(ii) In no event will Personal Data shared under this Addendum be used for commercial purposes (including by any third party), without the consent of such Data Subject having been obtained. The Agencies recognize that the provision of Personal Data to other entities for the purpose of facilitating the distribution of cash based assistance is not considered as a sharing of Personal Data for commercial purposes.

(iii) Any third party data sharing will be based on a contractual agreement with the third party to implement or monitor programmes in furtherance of the purposes for which the data was shared. The contract will stipulate that such Personal Data will not be shared onward with other entities (other than for technical processing to perform the third party's contractual obligations, approved by the receiving Agency). Each Agency will share Personal Data with third parties only to the extent compatible with its respective Data Protection Framework. In case of serious concerns relating to such third party, the requested Agency will provide information that substantiates the concern.

(iv) As soon as possible after the requesting Agency has determined a new third party with whom it wishes to share such Personal Data, the requesting Agency will inform the sharing Agency about such new third party and paragraph (iii) will apply.

(v) Under no circumstances may Personal Data transferred under this Addendum be disclosed, either directly or indirectly, by the Agencies or any contracted third party to agents or authorities of States which could represent a risk to the Persons of Concern.

5.3.4 Data Breaches

Should an Agency become aware of a Personal Data Breach in respect of Personal Data shared under this Addendum, it will inform the other Agency of the Personal Data Breach as soon as practicable upon becoming aware of it and provide a reasonable summary of the details thereof. Both Agencies will perform the required actions in line with their respective Data Protection Framework, including informing the Data Subject where required. The Agencies will cooperate to take joint mitigating measures without undue delay to ensure the protection of the Data Subject.

5.3.5 Addressing issues arising following the sharing of Personal Data

The Agencies acknowledge that there is a mutual interest in ensuring good data practices following the sharing of Personal Data under this Addendum. Accordingly, if Personal Data is used in a manner inconsistent with the purposes for which it was shared (unless agreed by the Data Subject); or if facts are discovered which raise significant data protection concerns (including a Data Breach) after sharing, the following will apply:

(i) the Agencies will mutually inform each other at the country level and will consult on the best course of action taking into account data protection concerns and operational requirements.
(ii) If, after a reasonable period of time (not less than four weeks) one party determines that the course of action proposed by the other party is not satisfactory, then such party may submit a written request to the other party proposing a course of action, failing which the Escalation Process in Section 7 will apply.

5.4 IT security relating to Personal Data

In addition to the general IT security measures set out in Section 6.4 below, the Agencies will take all possible measures necessary that Personal Data is kept secure – technologically, physically and organizationally – and must be protected by reasonable and appropriate measures against unauthorized modification, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer. Special considerations should be taken for Personal Data security related to devices, including mobile devices, containing Personal Data. The security of Personal Data should be subject to each Agency's respective Data Protection Framework.

SECTION 6. GENERAL PROVISIONS RELATING TO THE PROCESSING OF ALL TYPES OF DATA

The Agencies agree to comply with the following obligations with respect to all sets of Personal Data, Non-Personal Data and Information shared or to be shared pursuant to this Addendum.

6.1 Collaboration with respect to efficient data sharing and quality of data

When sharing Data with the other Agency pursuant to this Addendum,

(i) in the spirit of efficient and timely response, the requested Agency will set out the timeframe for sharing the requested data in a way to enable the requesting Agency to fulfil the purpose in a timely fashion;
(ii) the sharing Agency will provide the requested Data within the timeframe agreed in response to the request;
(iii) the sharing Agency will provide any requested data together with the Metadata identified in Annex 1;
(iv) the sharing Agency will notify the receiving Agency about any flaws, gaps or other challenges associated with such Data Set and will promptly provide any updates of the shared Data Sets; and
(v) the receiving Agency will promptly notify the sharing Agency in case of any inconsistencies or challenges in Data Sets received.

6.2 Anonymized Data

6.2.1 Where any type of Non-Personal Data is derived from Personal Data, it could in certain circumstances pose risks to certain categories of Persons of Concern. The Agencies therefore must endeavor to ensure:

(i) that the sharing and/or publication of such data cannot lead to the re-identification of Data Subjects, or otherwise enhance vulnerabilities, expose individuals or groups to harm, or jeopardise their protection. If the country offices of the Agencies determine jointly that the risk of re-identification is reasonably likely to materialize, the Anonymized Data should be considered as, and handled as, Personal Data in accordance with the terms of this Addendum (including Section 5); and
(ii) that the data sets do not divulge the actual location of small or at risk groups, for example by mapping data such as country of origin, religion or specific vulnerabilities to the geographical coordinates.

6.2.2 In situations where the sharing, publicizing or further processing of Anonymized Data is likely to pose risks to Persons of Concern, the Agencies' country offices will identify potential risks and mitigating measures prior to further processing.

6.2.3 If the Agencies cannot agree on the likelihood of the materialization of these risks they will utilize the escalation process outlined in Section 7.

6.3 Information security

6.3.1 **IT security of data systems and other practices.** UNHCR and WFP will, in accordance with their internal policies, implement comprehensive data security practices comprised of procedures to protect ICT (Information and Communications Technologies) assets and resources; provide robust information and records management; and control access to offices premises and facilities. Comprehensive data security practices should also include physical and electronic file management procedures, secure disposal of data, procedures for safe data transfers, minimum standards for portable electronic devices and password use, and privacy-by-design for new tools and systems. These measures must take into account the threat posed by malevolent external actors, insider threats, negligence, third-party relationships and natural and man-made hazards.

6.3.2 **IT security of data transfer.** Data should be transferred in machine-readable, encrypted, electronic formats such as Secure File Transfer Protocol (SFTP) or Secure Web Services, whenever possible. The specific modalities for data sharing will be decided by WFP and UNHCR at country level. Due consideration needs to be taken to identify the safest modality of data transfer, in line with the principles of confidentiality and data security stated above.

6.3.3 **IT security of partners**

(i) Cooperating partners. Each Agency will oblige any cooperating partner to establish and maintain appropriate technical and organizational measures against accidental or unlawful destruction, accidental loss, alteration or unauthorized disclosure to Personal Data in compliance with best industry standard or as agreed with the relevant Agency.

(ii) Commercial service providers. When using commercial service providers, the type of information security features that may be appropriate will vary according to the service provided (communications, data storage/ cloud services, survey tools etc.), i.e; ISO 27001 standards, cloud standards, bulk SMS standards, encryption standards, and financial services standards. In practice, each Agency will:

a) use approved corporate tools where available;
b) only procure the services of reputable service providers with industry standard information security features;
c) ensure that data protection, information security, and (if applicable) model contractual clauses are included in Requests for Proposals and assessments of potential service providers; and
d) verify the adequacy of the data security provisions takes before any Personal Data of is transferred.

6.4 Interoperability of systems

6.4.1 While maintaining the independence of each Agency's internal data management systems, the Agencies will work to achieve interoperability of specific functions of their respective systems to ensure efficiency and effectiveness of data sharing and assistance management in ways that are accessible by multiple partners and secure in terms of data privacy and protection.

6.4.2 The Agencies will, through the Joint Data Sharing Support Group (Section 8):

(i) agree on technical mechanisms to reach the system interoperability;
(ii) agree on technical data exchange standards;
(iii) specify the systems of record that are the sources of data to be exchanged; and
(iv) agree on standards with respect to the Non-Personal Data, such as data classification standards, geo-location standards (to be harmonized with the IASC Common Operational

Datasets (CODs) where possible and to use standardized hierarchical administrative boundaries and/or p-codes), project classification data.

6.4.3 Finally, the Agencies will develop modalities for synchronization of their data management systems with respect to the data covered by this Addendum.

SECTION 7. ESCALATION PROCESS FOR THE RESOLUTION OF ISSUES WITH RESPECT TO THE SHARING OF PERSONAL DATA, NON-PERSONAL DATA AND INFORMATION

7.1. The Agencies will endeavor in the spirit of cooperation under this Addendum to settle any disagreement or other dispute arising out of or relating to a request through amicable negotiations, including through consultation with the Joint Data Sharing Support Group (Section 8) and/or through assistance of the managerial level of the Agencies' respective country operations.

7.2 If any of the following occurs:

(i) a request is rejected in writing;
(ii) a response is not provided within one week from the date of the request; or
(iii) the requested Agency suggests an unreasonable time frame for data provision; or
(iv) the requested data is not provided within the timeframe indicated in the response to the request; or
(v) if any other disagreement or other dispute arises in this respect; or
(vi) upon receipt of Personal Data, Personal Data is used in a manner inconsistent with the purposes for which it was shared (unless agreed by the Data Subject); or
(vii) if facts are discovered on the use of Personal Data which raise significant data protection concerns (including a Data Breach); or
(viii) if country offices cannot agree on the likelihood of the materialization of risks of sharing Non-Personal Data (as per Section 6.2),

an Agency may submit such matter to the Regional Director of their corresponding regional bureau/office for resolution within one week or as otherwise agreed. The Agency escalating the issue will provide a substantiated description of the disagreement or dispute and, if applicable, accompanying evidence, such as the data sharing request, any negative response and, in the case of Personal Data contained in Annex 1, evidence for any valid reasons raised pursuant to Section 5.2.1(vi).

7.3. In the event that the Agencies' regional bureaus fail to resolve such disagreement or other dispute within one week or as otherwise agreed, such issue will be referred to the respective Directors of Programme (in Headquarters) for final settlement within one further week or such time as otherwise agreed.

SECTION 8. JOINT DATA SHARING SUPPORT GROUP

For support with the implementation of this Addendum and its Annexes, the Agencies will set up a Joint Data Sharing Support Group.

8.1 The Joint Data Sharing Support Group will be composed of, but not limited to, Data Protection, Information Security, Information Management, Identity Management functions within both Agencies.

8.2 The Joint Data Sharing Support Group will provide timely support with respect to any issues arising in the context of this Addendum. The Joint Data Sharing Support Group will determine terms of reference to include management of the implementation of this Addendum, e.g. by setting up a work plan for the technical aspects of this Addendum, namely data exchange, systems interoperability (as identified but not limited to Section 6), standard information services, biometric services, carrying out joint impact assessments, and other technical matters.

8.3 The Joint Data Sharing Support Group will meet whenever an issue is referred to it for consultation ad hoc upon request of one Agency, and regularly (at least once per year) for lessons learned and improvements / changes of the procedures set out in this Addendum.

8.4 Joint Data Sharing Support Group will operate by consensus of all members.

SECTION 9. GENERAL PROVISIONS

9.1 This Addendum will come into effect on the date of its signature by both Agencies. It may be modified or terminated at any time by mutual written agreement.

9.2 All other provisions of the Global MoU (as amended) will, except as otherwise expressly changed or modified by this Addendum, continue to remain valid and applicable.

9.3 Nothing in this Addendum or in any agreement or other document entered into or issued in connection with this Addendum shall be deemed a waiver, express or implied, by WFP or UNHCR or by the United Nations or the Food and Agriculture Organization of the United Nations of any privileges or immunities enjoyed by them pursuant to the 1946 Convention on the Privileges and Immunities of the United Nations, the 1947 Convention on the Privileges and Immunities of the Specialized Agencies, customary international law, other relevant international or national agreements, or under domestic law.

Filippo Grandi
United Nations High Commissioner
for Refugees

Date: 17 Sept. 2018

David Beasley
Executive Director
World Food Programme

Date: 17-9-18

Annexes

Annex 1 – Matrix of Personal Data, Non-Personal Data and Information

Annex 2 – Request Form for Non-Personal Data and Information

Annex 3 – Request Form for Personal Data