WFP World Food Programme

Field Level Agreement

WFP DATA PROTECTION CONDITIONS OF THE FIELD LEVEL AGREEMENT

These Data Protection Conditions ("**Conditions**") govern the processing of Personal Data under the Agreement. Any terms not defined herein shall have the meanings set out in other parts of this Agreement.

1. DEFINITIONS

1.1 "**Controller**" means the natural or legal person (including public authority, agency, NGO or other body) which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. For the purposes of these Conditions, WFP acts as the Controller of any Personal Data processed within this Agreement.

1.2 "**Personal Data**" means any information relating to an identified or identifiable natural person (each, a "**Data Subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data covers digital as well as non-digital information that is provided to the Processor or its Sub-Processors by or on behalf of the Controller or is obtained by the Processor or its Sub-Processors in connection with Processor's activities under this Agreement.

1.3 "**Process**" or "**processing**" (or any variation thereof) means any operation or set of operations that is performed on Personal Data, whether or not by automatic means, such as viewing, accessing, collecting, recording, organizing, storing, adapting or altering, retrieving, consulting, using, aligning, combining, blocking, erasing or destructing Personal Data. This also includes disclosing by transmission, anonymization, dissemination or otherwise making Personal Data available.

1.4 "**Privacy Rules**" means, as in effect from time to time, in connection with the processing of Personal Data, the applicable Controller data protection rules, principles and guidelines (ref. Executive Director's Circular OED 2024/002, as amended from time to time, and any related WFP policies) and, exclusively in respect of the Processor, also any data protection and information security laws and regulations applicable to the Processor and/or any sub-processors.

1.5 "**Processor**" means a natural or legal person (including public authority, agency, NGO or other body) which processes Personal Data on behalf of the Controller. The Cooperating Partner acts as the Processor of any Personal Data processed within this Agreement.

1.6 "**Privacy Incidents**" means any actual or reasonably suspected: (1) unauthorized access to or theft of Personal Data; (2) unauthorized use of Personal Data by a person with authorized access to such Personal Data; (3) unauthorized disclosure or alteration of Personal Data; (4) accidental or unlawful destruction of Personal Data; or (5) loss of Personal Data, in each case by the Processor or its Sub-Processors.

1.7 "**Representatives**" means, with respect to the Processor and any Sub-Processors, such party's directors, officers, employees, personnel, affiliates, who are involved in the implementation of the activities agreed upon under this Agreement with respect to Personal Data. The Processor shall assume full legal responsibility for acts and/or omissions of its Representatives and its Sub-Processor's Representatives in connection with these Conditions.

1.8 "**Security**" means technological, physical, administrative controls (including but not limited to policies, procedures, organizational structures, hardware and software functions) and physical security measures, the purpose of which is, in whole or part, to ensure the confidentiality, integrity and availability of Personal Data.

1.9 "**Sub-Processor**" means any Processor's contractors, subcontractors or agents, who contribute to the Personal Data processing activities of the Controller under this Agreement.

2. PURPOSES

2.1 WFP hereby authorizes the Processor to process certain types and categories of Personal Data as specified in the Agreement and/or instructed by WFP, on behalf of WFP. Such processing is necessary for the performance of the Agreement by the Processor. The Processor shall only process the Personal Data strictly needed to render the activities set forth in the Agreement and only during its duration, unless expressly otherwise agreed with the Controller in writing.

2.2 The Processor warrants that it has sufficient expertise and skills in conducting the specific data processing activities assumed under this Agreement, and that it has appropriate technical and organizational measures in place to comply with the Privacy Rules.

3. PROCESSING OF PERSONAL DATA

3.1 The Processor covenants and agrees to process Personal Data in accordance with the Privacy Rules and these Conditions. More specifically, the Processor shall: (i) act solely in accordance with the Controller´s written instructions to adequately perform the activities under this Agreement; (ii) only process Personal Data for the purposes of performing its obligations under this Agreement; (iii) shall not apply nor use the Personal Data for any other purposes than those set forth in this Agreement; (iv) shall under no circumstances use the Personal Data processed on behalf of the Controller for its own business purposes; (v) immediately inform the Controller in writing if, in its opinion, any instruction provided by the Controller infringes the Privacy Rules; (vi) immediately inform the Controller in the event of a breach of its obligations under these Conditions; and (vii) keep confidential, and not disclose, give access to or share Personal Data with any third party (including Sub-Processors) unless expressly authorized in writing by the Controller and only in compliance with the Privacy Rules.

3.2 As requested by the Controller, the Processor shall clearly and transparently inform Data Subjects about the processing of their Personal Data according to the instructions provided by the Controller and keep evidence of it in the manner specified by the Controller.

3.3 The Processor shall implement and maintain all the appropriate technical and organizational measures necessary to ensure the Security of the Personal Data that it processes to avoid its alteration, loss, or unauthorized processing or access, considering the state of technology, the nature of the Personal Data stored and the risks to which it is exposed, whether these are caused by human, environment, or nature. Security measures must be consistent with Privacy Rules, relevant international security standards and at least comply with the Information Security Appendix attached hereto.

3.4 The Processor must keep a written record of all processing activities performed on behalf of the Controller. That record shall contain at least (i) name and contact details of the Processor and its Sub-Processors for this specific Agreement; (ii) the types of processing activities performed on behalf of the Controller, (iii) purpose(s) of its processing, (iv) description of categories of Data Subjects and Personal Data processed; (v) where allowed transfers of Personal Data to a third country, and (vi) a general description of the technical and organizational security measures implemented.

3.5 The Processor shall communicate Personal Data to the Controller’s other Processors in accordance with the Controller’s written instructions.

3.6 The Processor shall not conduct any data transfer of the Personal Data processed on behalf of the Controller to a third country without prior written authorization of the Controller (including, without limitation, transfers relating to cloud-based services).

3.7 The Processor acknowledges that it has no proprietary rights whatsoever in the Personal Data processed by it.

4. SECURITY AND CONFIDENTIALITY

4.1 Confidentiality obligations as per Section 3.1 (vii) and this Section 4 shall prevail indefinitely, even after the expiry or termination of this Agreement. The Processor may provide access to Personal Data to its Representatives only to the extent such access is reasonably necessary for performing the Processor’s obligations under the Agreement, provided that: (i) such Representative is subject to obligations no less onerous than the requirements set out in these Conditions and the Information Security Appendix, and (ii) prior to granting any such access, the Processor has ensured such requirements and consequences of non-compliance are understood and followed by such Representatives.

4.2 The Processor shall ensure that Security is implemented, maintained and enforced to protect Personal Data from Privacy Incidents throughout the period of processing of Personal Data under this Agreement. Security shall, without limitation, be current and compliant with Privacy Rules, relevant industry standards and the Information Security Appendix attached hereto. Utmost care shall also be taken of physical security. The Processor shall evaluate its security systems regularly. This assessment shall be conducted in accordance with relevant international industry standards and best practices. The Processor shall promptly, upon the Controller´s written requests, provide the Controller with the results of such assessment(s).

5. REQUEST BY DATA SUBJECTS AND THIRD PARTIES

5.1 The Processor shall cooperate with the Controller in responding to any requests received from individuals who exercise their rights under Privacy Rules, including without limitation requests for access, correction, deletion, or any other rights, as applicable, regarding the Personal Data in the Processor's/Sub-Processor´s custody (each, an "Access Request"). This cooperation shall include, without limitation:

a) notifying the Controller within 5 business days of the receipt of such request by email detailing (i) type of request, (ii) date of receipt, (iii) impact and feasibility

b) consulting with WFP before taking any action as a result or in relation to such Access Request and

c) responding to such Access Request following the Controller's reasonable instructions.

5.2 Pursuant to the conventions, agreements and laws referenced in Article 15 of the General Conditions, Personal Data subject to this Agreement enjoys privileges and immunities. In the event that the Processor or a Sub-Processor receives a request or an order for the disclosure of Personal Data, in any form, from any government authority, the Processor shall immediately (but in no event later than 24 hours after receiving such request) notify the Controller in writing by electronic mail. Such notification must include a copy of the request or order. The Processor shall refrain (and shall be responsible for the Sub-Processor to refrain) from granting the requested access to or disclosure of the Personal Data unless and until authorized by the Controller in writing.

5.3 The Processor must appoint a Data Protection Officer (DPO) and/or a contact person and inform the Controller of his/her name, title and contact details.

6. NOTIFICATION OF PRIVACY INCIDENTS

6.1 The Processor shall train all its Representatives and Sub-Processors to recognize and respond to a Privacy Incident.

6.2 The Processor shall also take all necessary actions to prevent, contain and mitigate the impact of such Privacy Incident.

6.3 The Processor shall immediately conduct a reasonable internal investigation of the reasons for, and circumstances surrounding the Privacy Incident and shall implement preventive and corrective actions required to mitigate the impact thereof. The Processor must also collect and preserve all evidence concerning the discovery, cause, vulnerability, exploit, remedial actions and impact related to such Privacy Incident.

6.4 The Processor shall provide a written notice to the Controller promptly by email, but in no event later than twenty-four (24) hours after the Processor has discovered or become aware of a Privacy Incident, together with at least the following information:

a) A description of the nature of the Privacy Incident, including, wherever possible, the categories and approximate number of data subjects involved, and the categories and approximate number of Personal Data records involved; when (time of the Incident) and location of the Incident;

b) The name and contact details of the contact point where more information can be obtained;

c) A description of the possible consequences of the Privacy Incident; and

d) A description of the measures adopted or proposed to remedy the Privacy Incident, including, where applicable, the measures adopted to mitigate any possible negative effects.

In addition, it shall provide periodic written reports on the status/activities completed concerning mitigation and remedial actions related to each Privacy Incident, as well as any documents and/or information reasonably requested by the Controller related to such Privacy Incident. Where the information cannot be provided promptly and simultaneously, all available information shall be provided gradually but without undue delay.

6.5 The Processor shall refrain from any communication of or with reference to the Privacy Incident to: (i) any Data Subject whose Personal Data was or may have been affected; (ii) any data protection authorities to which the Processor may be subject; or (iii) the media and public at large, without having agreed such communication with WFP.

7. SUBCONTRACTING

7.1 Each Sub-Processor is a "subcontractor" as referenced in Article 16.7 of WFP General Conditions of the Agreement. The Controller may revoke its approval to retain a Sub-Processor at any time by notice.

7.2 The Processor shall ensure that any such permitted Sub-Processors are contractually bound to obligations that are substantively similar to, but not less than those imposed on Processor under the Agreement and these Conditions.

8. INDEMNIFICATION

8.1 The Processor shall indemnify and hold the Controller harmless, in the event any third party brings a claim against the Controller as a result of any negligent or intentional act or omission of the Processor (including its Representatives, Sub-Processors and their Representatives) with respect to any processing described in the Agreement.

9. TERMINATION, CANCELLATION AND EXTINCTION

9.1 Unless otherwise stated herein, upon the termination, cancellation or extinction of the contractual relationship between the Controller and the Processor, the latter must immediately return and/or delete all Personal Data processed by the Processor and its Representatives from any and all systems, devices and paper based- sources or any other source and shall send a written certificate confirming such destruction and deletion to the Controller once completed.

10. SURVIVAL

10.1 The provisions of these Conditions shall survive the termination or expiration of the Agreement in accordance with Article 17.4 of the WFP General Conditions.

INFORMATION SECURITY APPENDIX

This Information Security Appendix forms an integral part of the Agreement to which it is attached.

In addition to requirements set forth in the Agreement, the Processor shall:

1. Comply with WFP instructions on IT security and agrees to be subject to WFP information security reviews and/or audits, when requested.

2. Possess throughout the term of the Agreement:

2.1. A documented information security program based on one or more of the following industry standard information security frameworks: ISO, NIST, ISACA, COBIT; or

2.2. Implement the appropriate Security controls for the processing of Personal Data and provide WFP upon the signature of the Agreement with a description of such Security Controls, which shall include at least:

- a) The pseudonymization and encryption of Personal Data;
- b) The ability to ensure the ongoing confidentiality, integrity, and availability of processing systems and services;
- c) A process for regularly testing, assessing and evaluating the effectiveness of the Security controls implemented;
- d) The fast restoration of the availability of, and access to, Personal Data in the event of a Privacy incident; and
- e) The regular verification, evaluation and assessment of the Security controls. Such measures shall at least include mechanisms to:

    1. Enforce multifactor authentication for any user access to Personal Data;
    2. Ensure encryption of all devices including mobile devices, storage devices files and databases containing Personal Data and encrypt all communications between WFP and Processor, between Processor’s Representatives, between Processor and all third parties (including its Sub- Processors);
    3. Ensure that all files and databases containing Personal Data are backed up on a daily basis and paper-based information is duly secured in protected premises;
    4. Maintain a data governance framework according to the risks of the information accessed;
    5. Enforce system access controls, including granting user access, access recertification, revoking user access, administrative access and administrative user access management;
    6. Ensure that data access/ transmission/ input/ availability/ integrity/ segregation controls are in place; and
    7. Put physical access controls in place and ensure that physical security measures, in particular the ones targeted to protect paper based Personal Data and any other physical asset hosting Personal Data subject to the application of this FLA, are in place and are appropriate to the assessed security level of risk.