WFP World Food Programme | GPO Global Privacy Office

Field Level Agreements

Data Protection Conditions

Frequently Asked Questions

This FAQ is for WFP's country offices and Cooperating Partners (CPs) implementing Field Level Agreements (FLAs).

When are FLA Data Protection Conditions used?

Field Level Agreements Data Protection Conditions are embedded in FLAs and relate to projects where cooperating partners (CPs) collect/receive/use (process) personal data while working on WFP's programs and projects. When implementing an FLA, CPs play the role of **data processor**, acting on WFP's instructions. WFP is the **data controller**, working in alignment with the WFP Personal Data and Privacy Framework and deciding the means and purposes of data processing. In this role, WFP is also accountable for any wrongdoing, action or omission affecting beneficiaries.

What is WFP's Personal Data Protection and Privacy Framework?

It is a normative framework establishing comprehensive data protection and privacy standards for WFP when processing personal data. The Framework is shaped to WFP's mandate, following the most relevant international standards and best practices, and benchmarked with other UN data protection frameworks.

Who decides what information should be collected to implement the FLA activities?

WFP determines the data fields collected or used by the CP and for what purposes, based on operational needs, targeting criteria, and in compliance with the data minimization principle. Cooperating partners cannot collect different data than what has been specified by WFP.

What can CP do with this data?

Cooperating partners may only use this data to implement the specific FLA activities and achieve the objectives that have been agreed upon as part of the FLA. A CP cannot use data for any other purpose unless expressly agreed by WFP in writing.

Where should data be hosted?

Data may be hosted in WFP's own systems (e.g., SCOPE) or a CP's systems (i.e., LMMS, Kobo), depending on the case, and the instructions provided by WFP. Cooperating partners must follow the data security instructions provided in the data protection conditions and the related information security appendix. In any event, even if hosting data in its own systems, CPs may *only* use the data to implement the activities outlined in the FLA.

When collecting data, do CPs need to systematically collect beneficiary consent?

According to WFP's Personal Data and Privacy Framework, WFP may process personal data when at least one of the listed legitimate bases applies. The list includes vital interest, consent, and legitimate interest, among others. As data controller, WFP is responsible for determining which legitimate basis needs to be used in each case. If consent is used, WFP may instruct CPs to collect consent on its behalf. In these cases, WFP will provide CPs with the messages to be conveyed to beneficiaries.

Can CPs transfer data to any third party?

A CP may transfer data to third parties only if authorized by WFP and on the condition that the third party is acting as sub-processor and is contractually bound to obligations that are not less stringent than the FLA Data Protection Conditions. During the negotiation of the FLA, CPs are therefore invited to flag any issue related to this clause (e.g. internal audit rules requiring disclosure of data to auditors) to WFP in order to seek alternatives (e.g. transfer non-personal data) or accommodate the transfer subject to certain conditions (as the case may be).

What happens if a government asks a CP to provide access to WFP personal data?

Beneficiary data held by WFP as data controller is protected by the Conventions on the Privileges and Immunities enjoyed by WFP. This means that:

- Any systems, including soft and hard documents containing WFP data (including personal data of beneficiaries) are considered "inviolable," including when data is being stored in a CP's systems or premises.
- In addition, all data processed by or on behalf of WFP is part of organizational "archives" and "documents," regardless of where they are located or who holds them. As such, this data is part of WFP's "property and assets." Such data is inviolable, and it must be exempt from any type of search, requisition, confiscation, expropriation and any other form of interference, whether by executive, administrative, judicial or legislative action.
- This data is inaccessible to governments unless explicitly authorized by WFP.

Cooperating partners and their sub-processors should not share data with local authorities. If local authorities reach out to CPs or their sub-processors to demand access to data, the CP will immediately (no later than 24 hours after receiving the request) notify WFP in writing by e-mail. This notification must include a copy of the request or order. A CP shall refrain (and is responsible for ensuring that the sub-processor refrains) from granting the requested access to or disclosure of the personal data unless and until authorized by WFP in writing.

What are the mechanisms for data subject rights provided by WFP Data Protection and Privacy framework?

When a CP receives a data-related request from a beneficiary (regardless of the channel used to communicate the request) they should inform WFP immediately (and in any case within five business days of receiving the request). WFP is responsible for determining the mechanism for addressing data-related requests from beneficiaries. While a CP is expected to cooperate with WFP, it should not take any initiative without prior consulted and agreement with WFP.

What happens to data when an FLA expires?

A CP should return and/or delete all personal data from their systems, devices and paper based- sources or any other source and shall send a written statement to WFP confirming that data has been destroyed or deleted. During the negotiation of the FLA, CPs are invited to flag any issue related to this clause (e.g. internal audit rules requiring longer retention of data), to seek alternative solutions.

What should CPs do in case of privacy incidents (personal data breaches)?

A CP should immediately conduct a reasonable internal investigation and implement preventive and corrective actions to mitigate the incident's impact. A CP should immediately (and no later than 24 hours after discovering the incident) inform WFP. A CP should not disclose the incident to beneficiaries, any data protection authorities, media and the public at large, without prior agreement on the communication with WFP.

Is it requested that all ongoing FLAs be amended to integrate the data protection conditions?

An FLA amendment aimed at the integration of data protection conditions is recommended if personal data is processed as part of the current FLA implementation. The Global Privacy Office may provide support in deciding whether an amendment is needed.

What happens if a CP needs to use WFP's data to implement its own programs?

These FLA conditions apply when CPs act as WFP's cooperating or implementing partner. This includes implementing activities which are part of WFP's programs, on behalf of WFP. In the context of a CP's own programs, the CP may have different data-related needs related to data that WFP holds (e.g. targeting in same areas). In these cases, a CP may reach out to the WFP country office and start a separate discussion, unrelated to the FLA.

The Global Privacy Office is ready to provide guidance and answer any questions, comments, or concerns about data protection and privacy in WFP.

Contact the One-Stop Shop for privacy: ***Global.Privacy.Office@wfp.org***