Fighting Hunger Worldwide

WFP Guide to Personal Data Protection and Privacy

WFP
World Food Programme
wfp.org

Published in June 2016 by
the World Food Programme
Via C.G. Viola, 68-70, Rome 00148, Italy

WFP Guide to Personal Data Protection and Privacy

Principles and operational standards for the protection of beneficiaries' personal data in WFP's programming

WFP
World Food Programme
wfp.org

Table of Contents

1. Introduction

In carrying out its mandate, WFP processes a large amount of information, including personal data of its beneficiaries and prospective beneficiaries.

Protecting this information is a fundamental part of WFP's duty of care to those it serves. Breaches in confidentiality could have dire consequences for individual beneficiaries or beneficiary communities, ranging from abuse and ostracization to death.

These Guidelines have been developed for all WFP personnel involved in the processing of data concerning actual or potential beneficiaries. They cover data protection principles and the application of those principles. They also provide instructions on how to conduct a Privacy Impact Assessment, and include tools for use at HQ and in the field.

These Guidelines apply to all beneficiary and prospective beneficiary personal data. For purposes of clarity and to avoid repetition, all references to 'beneficiaries' include current and prospective beneficiaries. Similarly, references to 'beneficiary personal data' in this document include 'prospective beneficiary data'.

Key Definitions

Box 1
What is personal data?

Personal data is any information relating to an individual that identifies the individual or can be used to identify them.

A person can be identified directly from data such as their name, surname, and identification number, etc.

They may be identified indirectly from data that describes recognizable attributes, such as specific physical, physiological (including biometric and genetic), behavioural, mental, economic, cultural, or social characteristics.

International data protection laws typically distinguish between categories of personal data, depending on how strictly the information must be protected. These categories are defined as follows.

Personal Identity Information is any data that directly or indirectly identifies, or can be used to identify, an individual. It includes, but is not limited to the person's:

- Name
- Address
- Identity number
- Gender
- Age or date of birth
- Financial account numbers

Sensitive Personal Data is personal data that warrants even stricter security and confidentiality. It includes, but is not limited to the person's:

- Racial or ethnic origin
- Physical or mental health status
- Sexual orientation
- Political opinions or affiliations
- Religious or philosophical beliefs
- Criminal record
- Biometric data, such as photos, fingerprints, etc.
- Genetic information
- Membership of a trade union
- Ex-combatant status
- Refugee displacement status

In WFP, for the purpose of these Guidelines, and for consistency with WFP's Corporate Information Security Policy,[1] all beneficiary personal data is potentially sensitive and is considered as *strictly confidential*. Furthermore, such data will be considered as a '*vital record*' in line with proposed WFP Business Continuity definitions.

Anonymizing

Stripping or disguising information that could be used to identify an individual from a data set. Anonymizing is used to prevent identification of the individual either directly or by deduction.

1 http://docustore.wfp.org/stellent/groups/public/documents/cd/wfp274609.pdf

Biometric data

Data relating to unique physical, physiological or behavioural characteristics that has been recorded and can be authenticated digitally to identify an individual. Examples include iris and finger print scans, and facial recognition.

Data controller

The primary custodian of personal data. This may be an organization or an individual. The data controller determines the purposes for which, and the manner in which, personal data is processed. They retain ultimate responsibility for protection of the data even if they delegate use of the data to other organizations or individuals.

Data processing

Any operation or set of operations that is performed, either manually or by automated means, on personal data or sets of personal data. Processing includes data collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment and erasure or destruction.

Data subject

A term commonly used in data protection and privacy laws to mean individuals who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person. For the purposes of these Guidelines, the data subject is a WFP beneficiary or prospective beneficiary, and is referred to throughout the document as a ‘beneficiary’ or ‘beneficiaries’.

Encryption

A process of encoding messages or information in such a way that only authorized parties can read it.

E-transfers

Electronic cards issued to beneficiaries, which may be secured using biometric data, for in-kind food distributions, food and cash transfers. WFP is phasing these in to replace paper vouchers.

Informed consent

The freely-given and informed permission granted by the data subject to collect and process their personal data. Before granting permission, the data subject must understand: the intended purpose of this collection and processing; with whom this data may be shared; and any risks to their privacy that might stem from their data being collected and processed.

Tiered access

Role-based access to information. The minimum requirement rule stipulates that persons can only access information they require in order to do their job.

Rationale

Processing of data about beneficiaries is essential to planning and providing WFP food assistance. Registration and issuance of food-ration cards are instances of personal data processing. Other examples may be found in household surveys and beneficiary profiles, and in capturing still pictures and video images. For the purposes of programme implementation, WFP also shares personal beneficiary data with cooperating partners and/or service providers. Processing of personal data has legal, ethical and operational implications and must be considered within the broader framework of *data protection*, *privacy* and *human rights*.

Legal responsibilities

The individual's right to privacy is enshrined in various international legal instruments and principles, including the Universal Declaration of Human Rights.[2]

WFP needs to respect the right to privacy and the protection of personal data. In this respect, WFP's 2012 Policy on Humanitarian Protection[3] unequivocally requires that food and nutrition assistance be delivered with respect for human rights, and that food assistance should contribute to the safety, dignity and integrity of vulnerable people.

---

2 Article 12, 17 (1), 26 of the International Covenant on Civil and Political Rights; Article 8 of the European Convention of Human Rights; Article 11 of the American Convention on Human Rights; 1990 UN Guidelines concerning Computerized Personal Data Files; 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; 1980 Guidelines of the Organization for Economic Cooperation and Development (OECD) on the Protection of Privacy and Trans-Border Flows of Personal Data; 1995 European Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data; and Article 7, 12, 13 of the Universal Declaration of Human Rights.

3 WFP/EB.1/2012/5-B. Online at: http://documents.wfp.org/stellent/groups/public/documents/eb/wfpdoc061670.pdf

Ethical and operational issues

Processing of personal data carries inherent risks that are often unrecognized and unaddressed. Privacy breaches and the disclosure of data, whether intentional or unintentional, may have important ethical and operational repercussions.

The loss, theft or misuse of personal data may cause harm to the people WFP seeks to assist, as well as to WFP personnel. An individual whose personal data is unduly disclosed may be subjected to very serious abusive behaviours. Once a breach of privacy has occurred it cannot be undone, and it may adversely affect the beneficiaries for the rest of their lives. This is particularly true in armed conflict settings and other highly volatile socio-political situations such as dictatorships or ethnically biased conflicts.

Examples include:

- a former combatant hosted in an IDP/refugee camp may experience reprisals;
- beneficiaries belonging to an ethnic minority may suffer racial persecution;
- people living with HIV or who have survived Ebola Virus Disease may face stigmatization; and
- sexual violence survivors may become socially marginalized.

Loss or misuse of personal data may also result in a loss of confidence between the organization and its beneficiaries.

A lack of corporate standards and common understanding of data protection and privacy may also affect coordination and cooperation with WFP's donors, partners and other actors — for example, where the sharing of personal data is needed for humanitarian purposes requiring the assistance of a coalition of actors.

New challenges: e-transfers and biometrics

All these aspects of data protection and privacy become even more prominent with the increasing utilization of newer technologies, such as e-transfers and the use of biometrics. In e-transfers the personal data is more extensive than that gathered in conventional food distribution and is necessarily shared with, or generated by, commercial partners who assist, for example, in the distribution of cash via new technological means.

Because biometric data derives from characteristics of the human body, beneficiaries may consider its collection to be an affront to their human dignity. They may object to or resist collection on the basis of individual, religious or sociocultural factors. Likewise, use by WFP of non-traditional VAM survey tools (e.g. voice and SMS data collection) may also provoke concerns.

WFP's 2012 Policy on Humanitarian Protection[4] provides a framework for a more principled use of personal data. The policy specifically calls for guidance and systems for managing protection-related information, including sensitive personal data. Other WFP documents referencing data protection issues include WFP Corporate Information Security Policy,[5] WFP Directive on Information Disclosure,[6] and WFP Records Retention Policy.[7]

4 https://www.wfp.org/content/wfp-humanitarian-protection-policy, pp 17-18

5 http://docustore.wfp.org/stellent/groups/public/documents/cd/wfp274609.pdf

6 http://docustore.wfp.org/stellent/groups/public/documents/cd/wfp220970.pdf

7 http://docustore.wfp.org/stellent/groups/public/documents/cd/wfp089773.pdf

Box 2
WFP's Policy on Humanitarian Protection

(WFP/EB.1/2012/5-B/Rev.1)

WFP contributes to humanitarian protection by designing and carrying out food assistance activities that do not increase the protection risks faced by the crisis-affected populations receiving assistance, but rather, contribute to the safety, dignity and integrity of vulnerable people.

In line with the IASC definition of protection* WFP recognizes that protection is rights-based and founded on the relevant bodies of law, including human rights, humanitarian and refugee law

* IASC definition: 'Protection broadly encompasses activities aimed at obtaining full respect for the rights of all individuals in accordance with international law — international humanitarian, human rights, and refugee law — regardless of their age, gender, social, ethnic, national, religious, or other background'.

All WFP personnel[8] are duty-bound to ensure the confidentiality of beneficiaries' personal data. This applies to internal communications between WFP offices, and to those with third parties.

For effective implementation of these Guidelines, ideally the following measures should be developed.

[8] This includes, but is not limited to: international professional and general service staff members, consultants, interns, volunteers, locally-recruited staff members, interpreters, UN volunteers, persons recruited on Special Service Agreements (SSA) and Service Contracts (SC). It also applies to personnel on loan, secondment and exchange from UN Agencies, and to personnel from other organizations, including NGOs that are providing services for WFP. All individuals cited above, will be referred to as 'personnel' in the context of this guidance.

- A **Data Protection Officer (DPO)** role should be established at HQ. The DPO would be responsible for:

    i. overseeing effective and harmonized compliance with data protection principles, and implementing these Guidelines;

    ii. identifying, with all relevant stakeholders, effective responses to data protection breaches; and

    iii. coordinating with other UN agencies on data protection-related matters.

- A **Data Protection Focal Point (DPFP)** should be identified at each Country Office. Each DPFP would be responsible for:

    i. ensuring that Privacy Impact Assessments are conducted;

    ii. advising the Country Office on how to meet the standards set out in these Guidelines; and

    iii. coordinating with the DPO.

- WFP should ensure that:

    i. all personnel handling beneficiary personal data are familiar with the contents of this Guideline;

    ii. appropriate training is provided; and

    iii. appropriate IT security measures are in place.

Objective, Scope and Audience

The **objectives** of these Guidelines are:

- Increased protection of beneficiaries' personal data and right to privacy
- Increased protection of beneficiaries' safety and dignity
- Stronger transparency and accountability towards beneficiaries
- Enhanced security and safety of WFP Personnel
- Responsible use of technological innovations and developments (compliance with the Guidelines often requires the implementation of appropriate technologies)
- Harmonization of personal data protection measures and procedures across the organization
- Enhanced coordination and cooperation with WFP's partners
- Effective risk management.

Their **scope** is limited to the processing, both manual and automated, of personal data of WFP beneficiaries and prospective beneficiaries. The Guidelines apply to all programme activities regardless of distribution modality.

The Guidelines do not address anonymized aggregated information and statistics. Nor do they cover processing of Human Resources personal data or information relating to NGOs/implementing partners, vendors, or suppliers.

These Guidelines are an internal document with an intended **audience** of

all WFP personnel at Headquarters and in the field when any processing of beneficiary data is envisaged. The Guidelines should also be used when sharing personal data with third parties, such as other UN agencies, cooperating partners or contractors.

How to Use the Guidelines

The core content of these Guidelines consists of five principles. These are set out in Section 2. Each principle is presented with a definition (in bold), followed by operational notes that explain the principle. Where needed, boxes provide further information: green boxes highlight in-depth operational considerations; blue boxes highlight special considerations or circumstances.

Section 3 illustrates specific application of the principles.

Section 4 provides instructions for conducting a Privacy Impact Assessment (PIA).

Section 5 contains a selection of tools, consisting of operational templates and checklists. These are provided to assist WFP in operationalizing the principles and taking key practical steps at the various stages of data processing. The tools include:

- **Self-Assessment Compliance Checklists** that will allow personnel to measure compliance with each of the elements described in Sections 2, 3 and 4 of these Guidelines

- **Minimum Standards for Exceptional Circumstances** that personnel may refer to when faced with operational constraints (e.g. sudden mass refugee influx) that do not permit WFP to apply a standard and thorough application of the principles

- **Model Consent Forms** that can be used to develop local templates

for obtaining informed consent and for responding to beneficiaries' requests for access to their data.

These Guidelines should be used in conjunction with, and are complementary to, other relevant WFP policies and guidelines, including: WFP HR Rules and Contracts, the Standards of Conduct for the International Civil Service,[9] the WFP Directive on Information Disclosure,[10] Corporate Information Security Policy,[11] and WFP Records Retention Policy.[12]

9 http://icsc.un.org/resources/pdfs/general/standardsE.pdf

10 http://docustore.wfp.org/stellent/groups/public/documents/cd/wfp220970.pdf

11 http://docustore.wfp.org/stellent/groups/public/documents/other/wfp009147.pdf

12 http://docustore.wfp.org/stellent/groups/public/documents/cd/wfp089773.pdf

2. Data Protection Principles

The five principles explained in this section shall govern WFP's entire personal data processing system — from data collection, through storage, adaptation or alteration, retrieval, consultation, use, and disclosure and dissemination, to erasure or destruction.

The principles laid out in these Guidelines are in line with the Guidelines for the Regulation of Computerized Personal Data Files adopted by General Assembly resolution 45/95 of 14 December 1990,[13] and have been recognized by other international organizations as general principles of data protection. Since the principles are interrelated, and often interdependent, they need to be interpreted and applied in an integrated and coherent manner.

Privacy Impact Assessment

Prior to data processing WFP shall engage in a **Privacy Impact Assessment (PIA)**. A PIA is a privacy-specific risk-benefit analysis aimed at weighing the probability of harm against the anticipated benefits, and ensuring that the benefits significantly outweigh the potential risks and that any identified risks are avoided or mitigated. This includes considerations for the safety of WFP personnel.

[13] http://www.refworld.org/pdfid/3ddcafaac.pdf

This is an activity that must be performed in the early stages of project design. Instructions are given in Section 4, Conducting a Privacy Impact Assessment.

Box 3
Summary of WFP's five principles of personal data protection and privacy

1. Lawful and Fair Collection and Processing

WFP shall collect and process personal data by lawful and fair means with the informed consent of the beneficiary.

2. Specified and Legitimate Purpose

WFP shall collect personal data only for specific, explicit and legitimate purposes and shall further process it in a way that is compatible with those purposes. If a secondary purpose arises that is not compatible with the originally stated purpose then beneficiary consent must be obtained for this secondary purpose.

3. Data Quality

WFP shall ensure that personal data sought and obtained is adequate, relevant and not excessive in relation to the specified purpose(s) of data collection and data processing. WFP shall take all reasonable steps to ensure that personal data is accurate and up-to-date.

4. Participation and Accountability

WFP shall ensure that beneficiaries are consulted about the processing of their personal data before and during all stages of such processing. Beneficiaries shall be enabled to access, verify, correct, update and erase their personal data.

WFP shall ensure confidentiality of beneficiary personal information and will take appropriate actions in the event of a data breach.

5. Data Security

WFP shall continue to implement appropriate physical, organizational and technological security measures to protect personal data against accidental loss and/or damage, unauthorized access, disclosure, modification and destruction, and to ensure continuous availability of WFP's application programs and data.

Principle 1:
Lawful and Fair Collection and Processing

WFP shall collect and process personal data by *lawful* and *fair* means with the *informed consent* of the beneficiary.

Operational notes

Lawfulness

In practice, this means that WFP is bound by the following rules.

- WFP shall always have legitimate grounds for collecting and using beneficiary personal data. WFP's mandate is the overarching legitimate purpose for the processing of personal data by the organization.

- Personal data should not be used in ways that jeopardize people's human rights (e.g. the right to life, freedom of movement, freedom of thought) or in ways that have unjustified or adverse effects on individuals concerned.

- People should not be exposed to harm, or undignified or discriminatory treatment as a consequence of personal data collection and processing.

- WFP should handle personal data in a way that the individual concerned would reasonably expect and would agree to.

The principle of lawfulness does not, in itself, imply that WFP must comply with national law. This is because such compliance may conflict with relevant principles of international law that apply to WFP.

In this regard it is important to note that WFP and other United Nations agencies enjoy certain privileges and immunities, including inviolability of WFP's records and archives under the 1946 Convention on the Privileges and Immunities of the United Nations[14] and/or the 1947 Convention on the Privileges and Immunities of Specialized Agencies.[15]

On the other hand, NGOs and other WFP partners and service providers must comply with applicable national laws. This is not limited to data protection laws; it applies also, for example, to anti-terrorism laws, financial services regulations, and conditions for operating mobile phone licenses in the country of operations. They may, therefore, be obliged to disclose personal data to the government or local authorities.

Country Offices must:

- check whether the host country is enforcing a national law on privacy and personal data;

- understand whether that is compatible with the present Guidelines; and

- assess potential risks deriving from it.

This shall be part of the Privacy Impact Assessment, and will require the involvement of the Data Protection Officer at HQ. Country Offices shall seek the advice of the Policy and Programme Division (OSZ) and Legal

[14] Article II, Property, Funds and Assets, Section 4 at: http://docustore.wfp.org/stellent/groups/public/documents/manual_guide_proced/wfp258386.pdf

[15] http://portal.unesco.org/en/ev.php-URL_ID=48887&URL_DO=DO_TOPIC&URL_SECTION=201.html , with reference to Article 57 of the UN Charter: http://www.un.org/en/documents/charter/chapter9.shtml

Office (LEG) at HQ, particularly before assuming any obligation that may impact on WFP's status or the safety of WFP's beneficiaries or personnel.

Fairness

WFP needs to be transparent with beneficiaries on what personal information will be collected about them and how such personal data will be used/processed.

Personal data may *not* be deemed collected or otherwise processed 'fairly' if the beneficiary has not been informed, or has been misled or deceived, as to who the data collector is or what the proposed use of his/her personal data is. Please refer to Section 3, Informed Consent.

WFP needs to ensure that people's dignity and safety are preserved. Interviews soliciting and collecting personal data should be conducted in a safe environment, taking into account social and cultural mores, and age-, health-, language- and gender-related factors and sensitivities.

For example, in some societies it might be necessary to interview women and men separately; in others it may be more appropriate to interview household members together. Personnel should be trained in basic protection standards before conducting such interviews.

In order to avoid unnecessary and potentially harmful intrusion into people's private lives, WFP should limit data collection to the minimum necessary. ('Need-to-know' and 'data minimization' are explained below in Principle 3: Data Quality.)

In particular, in compliance with the Policy on Humanitarian Protection,[16] WFP and partners should refrain from collecting any information on individual protection incidents, such as cases of violence or abuse, unless

[16] http://documents.wfp.org/stellent/groups/public/documents/eb/wfpdoc061670.pdf

the information is necessary in order to:

- fulfil the specified legitimate purpose (see Principle 2);
- fulfil the obligations to contribute to people's safety and dignity; or
- monitor the corporate protection indicators, as set forth by WFP's forthcoming Corporate Results Framework.

If WFP personnel come across protection-sensitive information related to specific protection incidents, personnel may refer a person in need of assistance to a trusted service. This might be a protection-mandated NGO (e.g. Save the Children) or a UN agency (e.g. UNHCR or UNICEF) that provides clinical, legal, psychosocial or security services in the area where the affected person lives.

Referrals should only be made after WFP has mapped available service providers and established which can be trusted to provide services (including data protection) in accordance with international standards. Where mechanisms for referring protection cases to protection actors are in place, these can be used to pass on information about a particular incident to the relevant organization for follow-up. Note, however, that this should only be done with the consent of the affected person.

Informed consent

At the time of collecting personal data WFP should, at a minimum, explain to beneficiaries:

a) what type of personal data needs to be collected;

b) the purpose for which it needs to be collected;

c) who will access their data;

d) who they can contact if they have a concern with regard to their data.

Doing so will enable beneficiaries to:

- understand the intended use of their data and to whom it might be disclosed;

- evaluate possible risks associated with their data being stored and potentially shared; and

- decide whether or not to release their consent.

This consent must always be obtained, whether explicitly or implicitly, depending on the circumstances (see Section 3, Informed Consent).

Principle 2:
Specified and Legitimate Purpose

WFP shall collect personal data only for *specific*, *explicit* and *legitimate* purposes and shall further process this in a way that is *compatible* with those purposes. If a secondary purpose arises that is not compatible with the originally-stated purpose, beneficiary consent must be obtained for this secondary purpose.

Operational notes

This means that the purpose of data processing should always be:

- **Specified**: the purpose is definite and not subject to the discretional power of users. For example, the use of biometric data — a highly sensitive type of personal information — should be limited to the stated purpose and should never be used or shared for any other purpose, including, for example, alleged national security measures.

- **Explicit**: the purpose is defined prior to data collection and notified to beneficiaries either before or at the time of data collection (see Principle 1: Lawful and Fair Collection and Processing).

- **Legitimate**: the purpose is determined by the need for WFP to achieve its project's objectives and intended outcomes. WFP's mandate is the organization's overarching legitimate purpose for collecting and processing of data.

- **Compatible** with the original specified purpose. Any purpose that may subsequently arise that was not originally envisioned should be

evaluated to ensure consistency and compatibility with the original specified purpose before any further processing can take place.

Personal data may be used for secondary purposes (meaning any purpose that was not originally envisioned) that were not previously made explicit to beneficiaries as long as these have a reasonable and direct connection to the original specified purpose. Extending the use of personal data for a secondary purpose relies on the assumption that beneficiaries would permit the use of their data for that secondary purpose, even if that was not spelled out at the time of data collection.

For example, a secondary purpose that is compatible with the original purpose could be the use of personal data to continue the provision of assistance to beneficiaries (e.g. from IREMOP to EMOP). Also, it is not uncommon to cross-check registration data of one project against data of another. This would be viewed as a secondary compatible purpose as it is part of the normal work that WFP performs to ensure eligibility for provision of assistance. Likewise, verification counting, in which WFP engages for monitoring and audit purposes, would be considered a secondary compatible purpose, if aimed at preventing multiple claims by individuals for the same assistance provision.

If, however, the purpose of the data collection changes to something incompatible with or disconnected from the original specified purpose, beneficiaries need to be informed about the new purpose and release their consent.

The advice of the DPO should be sought if there is any doubt about the compatibility of any proposed secondary purpose.

Principle 3:
Data Quality

WFP shall ensure that personal data sought and obtained is *adequate*, *relevant* and *not excessive* in relation to the specified purpose(s) of data collection and data processing. WFP shall take all reasonable steps to ensure that personal data is *accurate* and *up-to-date*.

Operational notes

This principle means that personal data that WFP collects/processes shall be:

- **Adequate**: of sufficient quality and quantity to meet the specified purposes. For example:
  - in a food assistance for assets (FFA) land reclamation programme, prospective beneficiaries should be asked whether they own the land;
  - in cash-based programming involving a commercial operator, people should be asked whether they possess an official ID card (often a prerequisite for bank transactions) and whether they are literate.
- **Relevant**: closely connected or appropriate to the specified purpose.
- **Not excessive**: limited to the minimum necessary in order to avoid unnecessary and potentially harmful intrusion into people's private lives (need-to-know basis or data minimization). For example, if

prospective beneficiaries are simply being assessed for general food distributions it might not be necessary to collect data about educational background.

- **Accurate**: detailed, true, ideally first-hand and, where possible, corroborated by different sources (e.g. ID, local government, community leaders, etc.). Incorrect recording of personal data may impact on assistance delivery.

- **Up-to-date**: personal data should be kept as current as possible. When personal data is received from a third party, WFP should have a mechanism in place to update the data if the third party amends their records. Likewise, if WFP updates data received from a third party, a mechanism should be in place to inform the third party of such changes. Giving beneficiaries access to their personal data, and correcting or updating it for them as necessary, will also ensure that data is as current as possible (see Principle 4: Participation and Accountability).

Box 4
Ensuring that data is not excessive: the practice of "data minimization"

Any personal data that WFP processes, whether obtained directly from beneficiaries or from third parties, should be collected strictly on a "need to know basis". That is to say that the information has to be essential to achieve only the specified purpose, and no more than that. No data should ever be collected "just in case" for future purposes that are not specific and made clear to the beneficiary before data collection. This is an extremely important aspect of data protection and privacy, commonly referred to as "data minimization".

To ensure that the practice of data minimization is followed, the following questions should be asked, and if the answer to any of these questions is NO, then that information should NOT be collected.

- Does WFP fully and clearly understand the purpose for which it is collecting data and the information requirements to fulfil that purpose?

- Is the information being collected absolutely necessary to fulfil the specified purpose?

- If an individual were to ask WFP to justify every piece of data being collected about them, could WFP do so?

If there is any doubt as to if the data to be collected is excessive in relation to the specified purpose, the DPO should be consulted for advice.

Principle 4:
Participation and Accountability

WFP shall ensure that beneficiaries are *consulted* about the processing of their personal data, before and during all stages of such processing. Beneficiaries shall be enabled to *access*, *verify*, *correct*, *update* and *erase* their personal data. WFP shall ensure confidentiality of beneficiary personal information and shall take appropriate actions in the event of a data breach.

Operational notes

Participation

Beneficiaries are entitled to participate in their own data processing. In other words, they have a right to have their voice heard before and during data processing. WFP shall do the following to facilitate this.

- Consult beneficiaries on the degree to which they are comfortable with the types of data that WFP plans to collect for the implementation of a particular project. In doing so, WFP should consult representative segments of the concerned population, taking into account age, gender, ethnicity, cultural and/or other possible diversity characteristics. This consultation should be part of the Privacy Impact Assessment (PIA).

- Consult beneficiaries on which mechanisms are most suitable for them to request information and access data held on them. This, too, should be done as part of the PIA.

- Put in place procedures for beneficiaries to request and obtain

information about:

- what personal data WFP or its partners have recorded about them;
- with which third parties that information is being/will be shared;
- for what purposes it is being/will be used; and
- how to proceed if they have a concern with regard to their data.

- Put in place procedures allowing beneficiaries to update, correct or delete their personal data. Updates or corrections might relate to changes in the household's composition or its revenues and properties. Deletion of personal data does not require that the beneficiary provides a justification. This is known as the 'right to be forgotten'.

Box 5
Access requests from beneficiaries

- Beneficiaries requesting access to personal data must be able to identify themselves and demonstrate either:
  - that they are the data subjects; or
  - that they are legally authorized to access data on behalf of the data subject.

  Parents, tutors, guardians, legal representatives, or persons with power of attorney can request access on behalf of minors and people prevented by disability or debility from being able to request access themselves.

In all decisions affecting children, the best interest of the child is paramount. Access may be denied if WFP has sufficient reason to believe that persons requesting access are acting contrary to the best interest of the child (see Box 15).

- In case of a request to change/correct personal data held by WFP, e.g. because it is inaccurate, incomplete, unnecessary or excessive, WFP should request proof relating to the inaccuracy or incompleteness.

- Requests can be presented orally or in writing, and should be recorded using a standard form (see Section 5, Form B) or computer application.

- In the case of requests for deletions, the reasons for the request may be sought (for programme feedback purposes); however, the beneficiary is under no obligation to provide a justification.

  If, however, parents, tutors, guardians, legal representatives, or persons with power of attorney request data deletion on behalf of a child or other individual in their care, for protection reasons WFP should ask them to provide the reason for deletion.

  WFP should inform beneficiaries who request data deletion of any effects deletion may have on the assistance they receive. For example, it may not be possible to provide assistance if essential personal information is not provided.

Limitations to access requests from beneficiaries

- In cases where WFP has strong grounds to believe that requests are fraudulent, WFP may choose to restrict access to the data. Restrictions can also be applied to ensure:

- the protection of the beneficiary's safety, dignity and fundamental rights, or the rights of other people, such as WFP or partner personnel;

- WFP's overriding operational needs and priorities; and

- the prevention, investigation, detection and prosecution of serious criminal offences.

Conditions of disclosure to beneficiaries

- Only copies of documents should be shared (originals should remain with WFP).

- A note for the file should be added to the personal data record. The note will indicate date of disclosure, type of information disclosed, to whom it has been disclosed (data subject, authorized legal representative of the data subject), and the type of request (access, update, amendment or erasure).

- If a request is not granted because one of the above restrictions applies, reasons for such refusal should be added to the personal data record.

- WFP should respond to such requests within a reasonable time in a manner and language that is understandable to the beneficiary or legal representative of the beneficiary.

Box 6
Setting up mechanisms for requesting information on and/or correction/deletion of beneficiaries' personal data

Simple mechanisms should be established to allow beneficiaries to request information on their personal data held by WFP or its partners, as well as to correct, update, or erase this data. These mechanisms, all of which would be governed by these Guidelines, could include the following.

- Providing beneficiaries with contact details of the relevant WFP Sub and Country Offices (addresses, telephone numbers, e-mail addresses). Data Protection Focal Points (DPFP) should be considered for this purpose. If a DPFP is not available then special focal points may be appointed for this purpose at Sub- and Country-Office levels, as well as among cooperating partners.

- Feedback desk at the project site.

- Using existing hotlines and complaint boxes. Some cooperating partners may have put in place hotlines or informal boxes to enable beneficiaries to lodge complaints, and to provide and receive feedback about WFP's programmes. These mechanisms could also be used to request information and request corrective actions on personal data.

A Data Access Request Form (see Section 5, Form B) may be used for processing requests.

Accountability

When WFP processes personal data of its beneficiaries it has a duty to safeguard the confidentiality of their personal data. WFP also has a duty to safeguard the confidentiality of personal data obtained from any third-party organizations that have entrusted WFP with beneficiary data collected or otherwise obtained by them.

In the event of a data breach, WFP must take adequate measures for containment, issuing communications as necessary and learning from the experience to prevent any repeat event.

A ***privacy breach*** is an incident involving the unauthorized collection, use or disclosure of personal information. Unauthorized disclosures of personal information are the most common sources of privacy breaches and can occur when personal information is lost, stolen or inadvertently disclosed through human error. Circumstances that could lead to a privacy breach include:

- Loss or theft of equipment containing personal information (e.g., memory sticks, disks, laptops)
- Hacking of a network or computer
- E-mails sent to a wrong address or person
- Incorrect file attached to an e-mail
- Disposal of equipment containing personal information without secure destruction
- Insufficient controls in place to protect personal information in paper and electronic files
- Information faxed to a wrong number

- Breach of confidentiality by WFP personnel or third parties with whom WFP has shared beneficiary personal data

- Inappropriate postings to social media.

Box 7
Important Note

Personal data stored in a stolen or lost end user device (e.g. computer, mobile device, storage media) is assumed exposed to inappropriate access unless there is an approved and auditable means to prove otherwise.

In the event of a breach or suspected breach, containment and recovery steps should immediately be taken to the extent possible to halt the breach and/or reduce its effects. Specifically:

- To ensure a coordinated response, report any breach or suspected breach to the DPO, CO Data Protection Focal Point and Country Director. If at HQ, report it to the DPO and the appropriate Chief or Director. The following information, if known, should be provided:

  – The nature of the personal information involved (e.g. name, identification number, etc.)

  – The number (potential or actual) of individuals affected by the breach and who they are (e.g. beneficiaries from a specific community)

  – The possible scope of the breach (e.g. internal/external, who might have gained access to the personal information without

consent or authorization, length of time before detection of breach, etc.)

  - The date and/or location of the incident giving rise to the breach

  - When and how the breach was discovered.

- Assess any risks associated with the breach. In particular, potentially adverse consequences for individuals should be assessed with an indication of how serious or substantial these are and how likely they are to happen.

- Take mitigating measures and, depending on the severity determined by the risk assessment, consider the following steps prior to taking any further action:

  - Involve the Legal Office (LEG)

  - Involve the Communications Division (COM)

  - Involve the Inspector General and Oversight Office (OIG)

  - Involve the Human Resources Division (HR) for possible disciplinary measures

  - Inform beneficiaries (decision to be taken at an appropriate level of authority) and discuss with them possible mitigation measures to ensure their safety

  - Take all appropriate and feasible measures to ensure beneficiaries' safety

  - WFP may need to inform partners, if a data sharing agreement includes a requirement for notification in the event of a breach (check with LEG first).

If a third party with whom WFP has shared data experiences a privacy breach, WFP should ensure that the third party has performed the containment and risk assessment steps described above. Furthermore, WFP should analyse the third party's risk assessment and re-evaluate the impacts as necessary. WFP may also consider discontinuing the relationship with a third party depending on the circumstances leading to the breach. See Box 18 for guidance on Field Level Agreements (FLAs) for third-party data sharing.

Principle 5:
Security

WFP shall continue to implement appropriate *physical*, *organizational* and *technological* security measures to protect personal data against accidental loss and/or damage, unauthorized access, disclosure, modification and destruction, and to ensure continuous availability of WFP's application programs and data.

Operational notes

Personal data must be 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. This security must be subject to rigorous IT governance, controls, and auditability.

The most common data security vulnerability points are:

- **Networks** — as doorways for intrusions, introduction of viruses or malware, or interception of data in transit (e-mail, uploaded or downloaded data, etc.)

- **Data centres** — data storage systems compromised by unauthorized physical access, or by means of viruses or malware via a network or other source

- **End user devices** — local data storage on desktops, laptops, phones, or other data storage devices that could be compromised through loss,

theft, or unauthorized access

- **Office environment** — data held on paper records stored in an office or other depot, or being physically transported; or any other unsecured computers or storage devices.

Securing networks or data resident in data centres is largely the responsibility of WFP's IT organization. IT plays some role in the security of end user devices, but much of the practical responsibility lies with the end user. Securing paper records is almost always the responsibility of the end user.

Data security can be compromised in three main ways:

Type of security breach	Description	Example
Targeted theft	Intrusions that target the data or the hardware upon which it is stored by employing some method of circumventing any security measures in place, either physically or electronically.	• Hacking • Malicious software • Physical break-ins
Opportunistic theft	When equipment or paper records are left unsecured and accessible to unauthorized individuals.	• A thief takes advantage of encountering a laptop physically unsecured and unattended
Negligent/malicious insiders	When an authorized individual, either inadvertently or intentionally, reveals sensitive data or allows it to be revealed.	• Revealing a password • Leaving the computer with sensitive data visible • Leak from a disgruntled or corrupt employee

Personal data shall only be collected and processed once appropriate security measures are in place, and then only by authorized persons.

Box 8
Special considerations for data security

- Taking a device that contains beneficiary personal data out of the office or collating beneficiary data in the field presents considerable risk. Always ensure that such devices are secured through special security measures before being taken out.

- Be aware that deleting a record from a database or deleting a file does not necessarily remove that information from the computer (recovery tools can be used to restore the data). Electronic records should be destroyed with the advice and involvement of an IT officer.

- Be particularly vigilant with mobile devices when in public places. Aggressive thieves have been known to grab mobile devices right out of users' hands; if the device is on, data could be compromised.

Box 9
Special considerations when dealing with financial institutions

- When partnering with a Financial Service Provider (FSP) for a card-based intervention, ensure that the FSP is PCI DSS-compliant;

- PCI DSS is the Payment Card Industry Data Security Standard, a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM and POS cards.

- Defined by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud resulting from data exposure. Compliance is validated annually by an external Qualified Security Assessor for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire for companies handling smaller volumes.

Box 10
Physical security measures

- Ensure that paper records and portable electronic storage containing beneficiary personal data are stored in locked safes, shelves, drawers or rooms, and that these are kept in good repair.
- Restrict access to storage premises and server rooms to authorized personnel.
- Ensure that printed copies are appropriately destroyed as soon as they are no longer needed.
- Ensure that backup copies of the system are routinely made and stored in a separate, secure location.
- Protect the combination code of safes by restricting access and changing the code at regular, but not easily-predictable intervals.
- Paper records should be handled directly (not through couriers, mail, etc.)
- Store portable media in safe, secure locations
- Use devices such as Kensington Locks to tether equipment.
- Flag/highlight appropriate documents as Strictly Confidential.

Box 11
Technological security measures

- Ensure that all systems, networks, or hosting environments are configured according to WFP official policy and guidelines.
- Utilize anti-virus and anti-malware protection as per WFP policy.
- Manage passwords in compliance with WFP IT Security Policy.
- Use multiple levels of password protection — for example, one password to log on to a computer and another, different password to access an application that processes beneficiary information.
- Enrol mobile devices in a mobile device management system and enable mobile tracking to allow the device to be remotely wiped if it is lost or stolen.
- Use automatic time-out to invoke screen savers or to lock or log off computers.
- Use role-based access that provides different layers of data access to different personnel according to their job requirements.
- Use only secure internet connections; (Internet addresses [URLs] beginning with 'https:' are secure).

- Use data coding: replacing the identity of data subjects or other identifiable factors with labels or unconnected numbers and letters.
- Dispose of obsolete or non-functioning computers and other storage equipment according to WFP official policy.
- Avoid making copies for local processing of databases containing personal data.

Box 12
Organizational security measures

- Ensure that sufficient resources are allocated to enable all security measures to be implemented.
- Authorize access to personal data only to pre-defined roles/posts on a need-to-know basis with clear allocation of responsibilities.
- Ensure that responsibilities for data security are clearly allocated.
- Advice should be sought from LEG when negotiating confidentiality clauses or data transfer agreements.
- Ensure that all personnel are familiar with these Guidelines, particularly Data Protection Focal Points.

3. Specific Application of the Principles

Case study

Addressing resistance through sensitization/information in Bangladesh

At a camp where refugees had been resident for many years, the introduction of a new system of identifying eligible persons for benefits was met with strong resistance. Previously, refugees had to present a paper identification document to receive their benefits. The new system involved smart cards with the refugee's picture and fingerprints. The refugees understood fingerprinting as a form of giving consent, and they were apprehensive about giving a fingerprint for the beneficiary database lest their print be misused for other purposes, such as evidence of their agreement to repatriation.

WFP personnel held a number of mock distributions to demonstrate to the refugees how the new system would work — specifically, how fingerprints would be used to verify identities for the purpose of food distribution.

WFP also conducted an intensive sensitisation campaign for the smart card programme. This included meetings with refugee leaders, community meetings, household-level awareness sessions and distribution of flyers.

It was very important for WFP to coordinate closely with UNHCR and the Government. All three parties participated in meetings with the refugees and were present during the fingerprinting exercise. This also helped increase the trust of refugees.

Once the refugees understood exactly why fingerprints were required and how they were going to be used, their fears were allayed and the project was implemented with only a small percentage of the population declining to participate by withholding consent.

This is an excellent example of ensuring that consent is truly informed.

Informed Consent

Informed consent is the permission granted by an individual to collect and process his/her personal data after understanding and agreeing to:

- the intended purpose of this collection and processing;
- who this data may be shared with; and
- any risks associated with collection, processing or sharing of this personal data.

Beneficiaries need to be provided with enough information to allow them to judge and decide whether or not to grant consent. The information that

should be provided to beneficiaries in order to qualify their consent as 'informed' is listed in Box 13. **WFP must ensure that such consent is freely given.**

Once all the information has been provided, beneficiaries are enabled to decide whether or not to release their consent. This consent may be **explicit or implicit** depending on the circumstances (see Box 14).

- ***Explicit consent*** may be obtained:
  - in writing (see Section 5, Form A);
  - through a statement verbally released by beneficiaries, individually or collectively
- Consent may also be ***implicit*** as long as:
  a) the beneficiary has received all the required information (see Boxes 13 and 14);
  b) there is no evident obstacle to the expression of his/her free will (e.g. linguistic or cultural barriers);
  c) he/she has not put forward any objection after having been given the opportunity to do so (See Box 14).

The choice of whether to request explicit or implicit consent depends on the nature of the situation and whether WFP is in charge of the registration (see Box 14 for further indications).

Beneficiaries retain the right to ***withhold*** or ***withdraw*** their consent at any time. Ideally, it should be as easy to withdraw consent as to give it: to do that, appropriate mechanisms should be set up to enable beneficiaries to approach WFP (and/or cooperating partners) in an easy and safe manner and withdraw their consent (see Boxes 5 and 6).

WFP should inform the beneficiary of the implications of withholding or withdrawing consent. For example, a beneficiaries' refusal to provide the required information may make it impossible for WFP to provide assistance. Note, however, that WFP should endeavour to provide another form of assistance if one exists. For instance, it may be possible to offer a microfinance solution, which minimizes the extent of data sharing, instead of one involving commercial banks.

During the Privacy Impact Assessment, WFP should evaluate the potential degree of resistance to providing the type or types of personal information necessary for utilizing the envisaged transfer modality. People's concerns should be addressed when deciding the transfer modality, ensuring that all, or at least the overwhelming majority, would provide consent (see Box 14).

Box 13
Informed consent

Information to be provided

Ideally, for the consent to be truly informed, the following information should be provided:

- The identity and mandate of the data collector and data controller (e.g. WFP, cooperating partner, commercial agent)
- What types of personal data need to be collected/used
- Why such personal data are requested (specified purpose), including any other foreseeable purpose
- Who the data is expected to be shared with (e.g. financial service providers, mobile phone companies, other humanitarian actors) and that, in exceptional circumstances, the data may be shared with other parties in the context of government or national/international court or administrative proceedings, but only where the beneficiary's consent cannot be obtained and if in the best interest of the beneficiary
    - How to access, update, modify, correct or delete data and how to access complaint procedures
- The beneficiary's right to refuse to provide the information, and the implications of withholding consent — including the effect it may have on the type of assistance that may be rendered.

Beneficiaries should be given the opportunity to ask any questions, and receive answers to those questions before providing their consent.

How to provide the information

- Information should be provided, in writing or orally, in a manner and language that is understandable to the beneficiary.
- The easiest way to provide the information is through verbal briefings — individually or collectively, depending on the situation — allowing beneficiaries to ask questions.
- Leaflets, posters or other communications materials may also be provided to facilitate full understanding.

Box 14
Forms of consent

Explicit consent:

- Written consent: by means of written signature, thumb print or mark, prior to any processing (see Section 5, Form A)
- Video- or audio-recording the beneficiary's consent
- Oral statement provided by beneficiaries, either individually or collectively, indicating a clear understanding of the purposes and possible implications of data collection and processing.

Implicit consent:

- Implicit consent can be assumed if beneficiaries were provided with comprehensive information and they subsequently chose to proceed with providing WFP with their data.

  The following should be ensured:

  a) the beneficiary has received all the information;

  b) there is no evident obstacle to the expression of his/her free will (e.g. linguistic or cultural barriers); and

  c) he/she has not put forward any objection after having been given the opportunity to do so.

- A record should be kept in a form appropriate to the situation that the consent obtained was implicit, and not explicit.

Proxy consent:

- Consent may be provided by an individual (e.g. parent/tutor/legal guardian/person with power of attorney/legal representative) legally authorized to give consent on behalf of the beneficiary (see below segment on proxy consent)

What type of consent shall be sought?

- When WFP is in charge of registration, on the normal registration form that people are asked to sign, a box should be included stating that the person being registered provides his/her consent for the collection and use of their data for the purposes of the programme. This should be done as standard practice.

- In emergencies where WFP relies on local authorities or community members to compile registration lists and where only people's names and locations are collected, the preferred course of action will be to obtain other types of explicit consent (e.g. a verbal statement from beneficiaries, individually or collectively) or implicit consent.

- In situations where detailed or sensitive data is required (for example where data will be shared with third parties such as a government or a private service provider), separate explicit consent should be sought for the collection and use of personal data using a special consent form or video recording.

- In all of the above scenarios, information as outlined in Box 13 should be provided to ensure that consent is fully informed.

IMPORTANT: Records should be kept in writing on how information was provided to the beneficiaries and how consent was sought/obtained, and, in the case of proxy consent, from whom. In order to minimize instances of personal data and avoid duplication of files, these records should be noted in the same place where the personal data is recorded, either electronically or on paper.

Personal data should only be collected from individuals who are capable of providing it, or are legally required or authorized to give consent on behalf of others (***proxy consent***). This would apply to minors and to persons who, through disability or debility, are incapable of providing data. In the case of minors,[17] parents or legal guardians should provide consent on their behalf.

[17] According to the UN Convention on Children's Rights, minors are people under the age of 18.

In cases of proxy consent:

- WFP should ask for the legal evidence that the person signing/giving consent on behalf of the beneficiary has the legal capacity to give consent on his/her behalf.

- Where legal evidence is not available, WFP should seek witnesses in the community (e.g. neighbours, community leaders, relatives) who can confirm that the person is the legal or *de facto* representative of the beneficiary.

- As a last resort WFP must make a judgement as to whether data collection is in the best interest of beneficiary.

In all decisions affecting **children** it is paramount to understand and prioritize what is in the child's best interest. There may be instances where WFP has reason to believe that the parent/s or guardian/s are acting contrary to the best interest of the child. In such cases WFP shall seek the advice of a protection expert or, when available, a WFP protection advisor. Child participation should be fostered and the views and opinions of children should be respected at all times. Interviewers should be properly trained for the purposes of interviewing children.

In the case of **unaccompanied children**, depending on the age and the capacity of the minors, they should be directly informed and their consent should be sought. When doing so, special efforts should be made to:

- use appropriate and simple language when providing the information;

- test whether they have understood (e.g. through questions) — in particular, making sure that they understand which other entities may have access to their data, as well as what protection risks they may be exposed to as result of their data processing;

- seek the advice and the assistance, if relevant and possible, of a child protection expert while gathering consent.

Ultimately, WFP will make a judgement on whether processing the personal data of these children is in their best interest.

Box 15
Understanding what is in the child's best interest

Elements to consider when analysing what is in the child's best interest:

- The safety of the child
- Respect for the opinions of the child
- The age and maturity of the child
- Preservation of the unity of the family
- Preservation of the child's health
- The child's unhindered access to education.

In situations in which a beneficiary is **absent or not accessible**, it may be necessary to obtain proxy consent in order to collect their personal data. In such circumstances — whenever it is possible, safe, and culturally appropriate — steps should be taken to inform the beneficiary as soon as it is reasonably practical to do so and allow them to confirm/withdraw their consent. As a last resort WFP must make a judgement as to whether data collection is in the best interest of the beneficiary.

Other cases may arise in which, due to **practical or customary reasons**, people collect and provide the names of other people who are fully capable of giving their consent (e.g. community leaders providing the list of beneficiaries; husbands speaking on behalf of their wives). In these instances:

- WFP should judge whether beneficiaries are being denied their right to freely express their free will and, as a result, are being disempowered, marginalized or disrespected. If so, WFP should insist on collecting data directly from the beneficiary.

- Otherwise, WFP should demand and ensure that collectors obtain explicit or implicit consent, in compliance with the provision on informed consent.

- As a last resort WFP must make a judgment as to whether data collection is in the best interest of the beneficiary.

Third-party Data Sharing

Data sharing with third parties is often an essential element of WFP's operations. Beneficiary personal data may be received by WFP from third parties (inbound data). Beneficiary personal data may be transferred by WFP to third parties (outbound data).

Sharing personal data is one of the riskiest aspects of the whole data management cycle. If personal data were to fall into the wrong hands, beneficiaries' personal safety, and even their lives, might be at risk.

As part of a PIA at a project's outset, WFP should consider whether the organization envisages sharing beneficiary personal data with, or receiving it from, any third party (e.g. other UN agencies, cooperating partners, financial service providers). If so, WFP should consider what personal data is needed and for what specific and legitimate purpose.

All phases of the project should be considered from planning, implementation, through monitoring and evaluation. For example, in the context of cash-based transfer assistance, WFP may need to receive beneficiary personal data from another UN agency (inbound data) and transfer some of this data to a financial service provider (outbound data). Note that national laws differ as to how much information financial service providers are required to hold: in some jurisdictions providers must have very detailed information; in others an ID number may be sufficient.

In all cases, sharing of beneficiary personal data (whether inbound or outbound) shall be limited to the ***minimum necessary*** to fulfil the specified legitimate purpose(s), and will be done only with the ***informed consent*** of the person concerned.

Inbound data

WFP shall take reasonable steps to ensure that personal data received from third parties has been collected *in compliance with data protection and privacy principles*.

Third party to WFP (inbound)

Example 1.

UNHCR provides refugee data to WFP for enrolment in WFP's systems.

Example 2.

A cooperating partner uses SCOPE on WFP's behalf to register beneficiaries and then uploads the data to WFP's central database.

WFP often receives beneficiary data from third parties, including other UN agencies, NGOs and governments. In cases where WFP has contracted a third party to collect beneficiary data on WFP's behalf, Field Level Agreements (FLAs) or Data Sharing Agreements (DSAs) should prescribe how that entity operates with respect to these Guidelines. In these cases WFP remains the data controller with ultimate responsibility for protection of the data. In all other cases, where WFP receives data from a third party not acting on WFP's behalf, the third party remains the data controller and WFP will consequently have less control over the data collection process.

In any case, *at minimum* WFP should ensure to the best of its ability that this data has been lawfully collected in compliance with the principles in these Guidelines. In particular, beneficiaries need to be informed that their

data will be shared with WFP and they need to provide their consent to this.

If WFP becomes aware that consent has not been given, WFP should check with the third party if consent can be obtained. If that is not possible, WFP should attempt to inform the beneficiary that their data has been shared with WFP and for what purposes, and to obtain their consent, or at least give them an opportunity to object.

As a last resort, WFP must judge whether beneficiaries would be reasonably expected to accept that their data be shared with WFP and whether using their data is in their best interest. If so, WFP may proceed with the use of this data.

WFP should also ensure that:

- only the minimum data necessary to perform the required work is received;

- only authorized personnel have access to the data; and

- the data is kept for no longer than is strictly necessary to achieve the legitimate specified purpose, after which the data is returned to the data controller and/or destroyed.

See Box 16 for a comprehensive list of conditions to be met when receiving data from third parties.

Box 16
For consideration when receiving beneficiary personal data from third parties (inbound data)

- When receiving data from a third party WFP may be asked to sign a data sharing agreement or other agreement with the third party. The Agreement's conditions and measures therein may vary, depending on:

  – the third party's policy (UN agencies' requirements will be substantially similar to WFP guidelines but may still vary);

  – the requirements of local law (e.g. if the party transferring data to WFP is a local NGO); and/or

  – operational and technical needs and circumstances.

  All agreements should be referred to LEG and the DPO for advice.

- WFP should seek confirmation that the originating organization has collected the information in compliance with WFP's data protection and privacy principles by ensuring that:

  – the information was collected in a lawful and fair way;

  – the beneficiary was informed that their data will be shared with WFP and those that WFP may share it with, and gave consent for such sharing;

- the beneficiary was advised of the purpose for the collection of the data, and that WFP's use of this data is compatible with that stated purpose;
- WFP receives the minimum data required for WFP, or its partners, to perform the work to be done;
- the quality of the data is acceptable.

- There should be a mechanism in place for keeping data up-to-date and accurate (see Principle 4: Participation and Accountability).
- A mechanism for informing the originating third party when the data has been destroyed at the completion of the intended purpose should be defined.

Outbound data

WFP shall transfer personal data to third parties only with the *informed consent* of the beneficiary, for the *specified legitimate purpose*, and under the guarantee of *adequate safeguards* to protect the confidentiality of personal data, as well as the rights and interests of the beneficiary.

WFP to third party (outbound)

Example 1.

WFP provides personal data to an NGO for food distribution.

Example 2.

WFP provides personal data to a financial service provider as a component of a Cash and Voucher intervention.

Ad-hoc request from a third party to WFP (outbound)

Example 1.

A government/local authority requests personal data on beneficiaries for a specified purpose**.**

Example 2.

A non-partner NGO working in the same area asks for WFP beneficiaries' registration data to assist in their work.

As part of the Privacy Impact Assessment prior to data collection, WFP should analyse all flows of personal data from WFP to known and foreseeable third parties, and among third parties (e.g. from market vendor to financial services provider, or between third parties operating in partnership), in order to ascertain whether and where these flows create risks to beneficiaries. WFP should evaluate that the third party to whom data would be transferred can guarantee that beneficiary personal data would be protected in compliance with these principles and Guidelines.

Due to the possible impact on personal data protection, WFP should assess and be aware of laws and regulations that would apply to any third party (e.g. antiterrorism, anti-money-laundering, know-your-customer and other public safety laws.) See Principle 1: Lawful and Fair Collection and Processing.

Transfers of personal data to third parties shall only be done with the informed consent of the beneficiary, for a specified legitimate purpose, and under the guarantee of adequate safeguards to protect the confidentiality of personal data, as well as the rights and interests of the beneficiary. (See Principle 1: Lawful and Fair Collection and Processing). If possible, WFP should agree with the third party which security measures are best suited for protecting the confidentiality of such data.

Outbound data transfers must be limited to the minimum necessary to fulfil the specific and legitimate purpose(s) for which the beneficiary has given his/her consent. It is, therefore, important to discuss this with all relevant partners and to understand at the project's outset what personal data needs to be shared in each specific case.

When WFP plans to share beneficiary personal data with third parties (in particular when data sharing is, or is likely to be, systematic) it should agree with the third party in advance the specific conditions governing such data sharing. WFP's experience has confirmed that there is no universal template for this, and so data sharing agreements should be developed on a case-by-case basis. Country Offices shall seek the advice of the Legal Office in HQ when negotiating specific data sharing agreements.

See Boxes 17 and 18 for evaluation criteria and conditions for sharing data with third parties.

Box 17
Evaluation criteria for sharing beneficiary personal data with third parties (outbound data)

Formal criteria

- Entities requesting access to personal data must be recognizable, authentic and formally authorized to access personal data on behalf of the third party.

- The request must be in writing and indicate the:

  - intended specified purpose;
  - nature of data needed;
  - duration of proposed processing;
  - method of transfer to be used;
  - retention period;
  - method and proof of destruction; and
  - security measures in place.

- Beneficiaries must provide informed consent to data transfer, ideally prior to or at the time of data collection. When that is not possible, WFP should inform the beneficiary that their data is to be shared, with whom and for what purpose/s, and at least give the beneficiary the opportunity to withhold consent. As a last resort, WFP must make a judgment as to whether beneficiaries would reasonably be expected to accept the sharing of their data with the third party and whether using their data is in their best interest. If so, WFP may proceed with sharing this data.

Substantive criteria

- The request must be legitimate — i.e. aimed at performing an activity of humanitarian or protection nature — and it must comply with the key principles of international personal data protection law.

Even when the request is legitimate, WFP will have to evaluate the following:

- *Overall best interest of the beneficiary*: this is achieved when the beneficiary's safety, dignity and rights are preserved. This has to be considered the paramount evaluation criteria

- The third party's capacity to ensure confidentiality and, more generally, compliance with WFP's data protection principles, including adequate security measures

- Potential repercussions on the safety and security of WFP's personnel and/or personnel of WFP's implementing partners

- Potential repercussions on WFP's operations or reputation, e.g. loss of beneficiary trust in WFP as a neutral, independent, non-political organization.

Box 18
How to disclose personal data to third parties

- Before disclosing personal data to a third party, WFP should have an agreement with the third party that includes the:
  - specified legitimate purpose;
  - type of personal data needed;
  - prohibition of further use and disclosure, when appropriate;
  - duration of proposed processing;
  - retention period;
  - method of destruction, return or anonymization;
  - procedures to follow in the event of a breach; and
  - adherence to WFP's personal data protection principles.

  Draft agreements should be referred to LEG for advice and reported to the DPO.
- Data must be disclosed only on a 'need-to-know' basis. In other words, only the information necessary to meet the identified legitimate purpose should be disclosed.
- Only copies of documents should be shared. Originals should remain with WFP.

- All possible steps should be taken to avoid unrestricted dissemination, and the most secure method of transfer under the circumstances should be used (see Principle 5: Security).

- A note for the file should be added to the personal data records. The note will indicate date of disclosure, type of information disclosed, to whom and the specified purpose; and reasons for sharing/not sharing.

When data is both Inbound and Outbound

Sometimes the same personal data are subject to both inbound and outbound sharing processes. In such cases it is important to be clear as to who is the data controller and who is the data processor and what their respective responsibilities are. An example of this would be when WFP receives refugee data from UNHCR for the purpose of implementing a cash based transfer intervention requiring that WFP share that data with a financial services provider. In this example, UNHCR is the data controller and WFP is the data processor. When WFP in turn shares that data with the financial services provider, WFP becomes the data controller, but with regard only to the relationship with the financial services provider.

When WFP receives data from a third party (who remains the data controller) that party must grant approval to WFP to provide this data to any fourth party, including the specific purpose for sharing the data, and this should be documented in the Data Sharing Agreement between WFP and the third party. In addition, the beneficiaries must have given their consent to the data controller for their data to be shared with WFP and any fourth parties.

It may be possible that the third party or WFP itself has concerns about the fourth party's capacity and willingness to ensure the data is protected to the

expected standard. In such cases, it is recommended that WFP and the third party jointly carry out a Privacy Impact Assessment of the fourth party in order that all risks and mitigation strategies are understood and agreed to by both parties. At minimum, WFP should share the results of their own assessment with the third party and this should be appended to the Data Sharing Agreement.

Concrete disclosure situations: how to evaluate a third party's access request and beneficiaries' best interests

When receiving a request for access to beneficiary personal data from any third party (whether from a government, service provider, vendor, NGO, donor, or other) the principles described in these Guidelines ***always apply***.

Among the substantive criteria underpinning the disclosure of personal data to third parties are: the legitimacy of the third party's request, and the beneficiaries' best interest (see Box 17). ***These two criteria may sometimes conflict with each other, which can make the request difficult to evaluate. As a general rule, beneficiaries' best interests take precedence over even a legitimate request.***

Also, when faced with a third party request for access to beneficiary personal data, WFP must understand where the request comes from, the purpose of the request, and what type and amount of information is needed to fulfil that specific purpose.

It may transpire that the third party only needs to receive general information, as opposed to data that identifies or describes individuals. For instance, a donor may have a legitimate interest in knowing how many beneficiaries have received assistance, but they do not need individual beneficiaries' personal details. In other scenarios, it may be that only very limited data is needed in order to comply with local regulations.

In all cases, when a third party requests disclosure of beneficiary personal

data, LEG shall be contacted for advice before WFP responds to the request. This is to safeguard against putting beneficiaries and WFP personnel at risk, and against inadvertently waiving WFP privileges and immunities.

Below are some examples of requests that may be presented to WFP, with advice on how they should be dealt with.

Governments of host countries

Governments of host countries may approach WFP requesting access to personal data. In this case, the grounds for legitimate interest may be national security, public safety, public health, prevention or suppression of criminal offences, or other reasons necessary for the functioning of a democratic state (e.g. triangulation of beneficiary lists with electoral lists).

WFP fully recognizes states' sovereignty; however, recognition does not translate into unrestricted and automatic disclosure of personal data. Again, the purpose of the government's request must be balanced with the paramount protection interest of the beneficiary.

In all cases, states must respect the absolute inviolability of WFP's records and archives under the 1946 Convention on the Privileges and Immunities of the United Nations[18] and the 1947 Convention on the Privileges and Immunities of Specialized Agencies. Advice must be sought from LEG and OSZ before responding to any such request.

Governments of country of origin

Only under rare and specific circumstances should WFP share any personal data on refugees with any state or non-state entity in the refugees' country of origin. Specific exceptions to this rule might include cases of voluntary

[18] http://docustore.wfp.org/stellent/groups/public/documents/manual_guide_proced/wfp258386.pdf

repatriation, but in any instance data sharing must always be coordinated through UNHCR. In all cases, safety considerations should always prevail. Advice must be sought from LEG and OSZ before responding to any such request.

International organizations

WFP has a general interest in cooperating with other members of the international community and with international organizations (UN organs, UN agencies, IFRC, Special Rapporteurs, Special Representatives and Representatives of the Secretary General). However, access to personal data remains subject to the existence of a specified purpose, consent of beneficiaries, and the supremacy of protection interests of beneficiaries.

If a relationship between WFP and an international organization is governed by a Memorandum of Understanding (MoU) or other agreement addressing confidentiality and personal data protection, such an agreement should form the framework of the decision. Otherwise, the request should be evaluated according to the criteria set out in Box 17.

The International Criminal Court and other authorities in the context of court or administrative proceedings

WFP may also receive requests for access to or disclosure of beneficiary personal information from international or national authorities in the context of court or administrative proceedings. Such requests could be made by an international judicial authority, such as the International Criminal Court (ICC), or other national, international or arbitration tribunals, by state authorities conducting administrative or legislative proceedings as well as by international or national law enforcement authorities (e.g. Interpol, police).

WFP may be asked to assist these entities in different ways, such as: providing documents or information in its possession; providing

information on facts and crimes of which it has become aware; or testifying at a trial. It is likely that these activities would require disclosure of personal data, and would therefore raise protection concerns.

As a general rule, whenever approached by any of the above mentioned authorities, and disclosure of personal information is foreseen, WFP shall seek advice from LEG and OSZ before responding to such requests, in order to ensure compliance with the 1946 Convention on the Privileges and Immunities of the United Nations and the 1947 Convention on the Privileges and Immunities of Specialized Agencies.

Non-governmental organizations

WFP maintains close working relations with NGOs, especially when these are cooperating partners. Due to the humanitarian nature of their work, NGOs normally have a legitimate interest to access personal data. However, requests should be strictly assessed according to the criteria set out in Box 17. NGOs are subject to local law requirements, including requests from local authorities. If there is any doubt as to the origin or legitimacy of the request, or if there is cause for concern about downstream requests for information by authorities, advice must be sought from LEG and OSZ before responding to any such requests.

Service providers

Case study

WFP experience in a country with heavily regulated telecoms sector

WFP engaged with a local telecommunications provider to provide SIM cards to enable an SMS delivery solution to a large refugee population. The service provider advised that they would be obliged to provide the government with the identities of the persons using these SIM cards.

WFP consulted with UNHCR and agreed that providing that information to the service provider might compromise the refugees and that an alternative method of achieving the same goal should be identified. It was decided that WFP itself should be the registered user of the SIM cards, and that WFP would manage the distribution and coordination of the cards directly with the refugees. About a thousand cards were distributed under this plan. However, this option was not ideal, and WFP soon realised that the organization was exposed to a great deal of institutional and reputational risk. It therefore sought other solutions.

It transpired that many beneficiaries had acquired their own mobile phones and SIM cards and had already provided their identification details to the service provider, which had, in turn, passed this on to the government. As these people had no concerns about this information being released, the intervention switched to using the refugees' personal phones and SIM cards.

Some individuals or entities (e.g. mobile service providers, banks) may be authorized to act on behalf of WFP during the life cycle of data processing. Therefore, they have an inherent legitimate interest to access personal data.

It is important to bear in mind that all national partners (e.g. NGOs, vendors, cooperating partners) are bound by domestic laws that may directly or indirectly impact on personal data protection.[19] That means, among other things, that what states cannot access through WFP may be obtained through other parties with whom WFP has shared data. It is therefore essential that WFP personnel are acquainted with the national laws of the host country and that these are factored into WFP's Privacy Impact Assessment.

Data sharing with service providers should always be governed by a specific contract or data sharing agreement that ensures, among other things, that service providers adhere to the principles outlined in these Guidelines.

Key elements to consider in the contract/data sharing agreement include:

- what data is necessary for the legitimate purpose;
- consent of the beneficiary;
- security measures in place;
- restrictions on processing (including data sharing with further third parties);
- retention period; and
- methods of destruction or return to WFP.

[19] These include laws on data protection, antiterrorism, anti-money laundering, know-your-customer (KYC), and banking regulations, etc.

Donors

Donor reports should not include any personal data. Donors may request how many beneficiaries or what categories of beneficiaries have been reached, but no personal data of beneficiaries should be disclosed. If a donor requests access to beneficiary personal data, contact LEG and OSZ for advice.

Media

Print and broadcast media entities

WFP should, in principle, not share personal data with the media. Requests from the media to access WFP's beneficiaries should be rigorously coordinated in advance with the Communications Division (COM) and evaluated according to the sensitivity of the case, the level of risk involved, and the protection interest of the individual.

WFP materials, including text, photos and videos, are protected by copyright. Permission to use or reproduce any WFP material must be requested through COM. It will only be granted on condition that these principles and Guidelines are adhered to and the material is used in accordance with WFP rules and policies.

WFP's official use of images (photographs, video, and digital footage)

WFP, in particular the Communications Division, often documents its activities through photographs and digital video footage of beneficiaries. All these activities require that beneficiaries are informed of the specified purpose and that they release their informed consent, either explicitly or implicitly (see Boxes 13 and 14). See Box 19 for further specific measures to observe when the media and/or use of images are involved.

WFP should explain to beneficiaries in a very simple and understandable way:

- the purpose for which the photograph or video is being captured;
- who will/might see the material (which means that the beneficiaries need to understand the global reach of the Internet and social media); and

- whom they can contact if they have a concern about their photograph.

Personal use of images (with particular regard to social media)

WARNING! The rules set out in this guidance also apply to photographs and videos taken by WFP personnel or contractors for non-official purposes. In particular, personnel should refrain from posting any photograph or video on any personal social media platform (Facebook, Twitter, YouTube, etc.) without getting explicit or implicit consent from beneficiaries (see Box 14 on explicit and explicit consent).

See Box 19 for specific measures to observe in situations involving the media and/or use of images, and Section 5, Communications Subject Release Form for obtaining beneficiaries' consent.

Personnel are directed to the WFP Guidelines on Social Media[20] which can be found on WFP*go*.

[20] http://go.wfp.org/web/communications/social-media-guidelines

Box 19
Specific measures when the media and/or use of images (official and personal use) are involved

When media reporting and the use of images are envisaged, the beneficiaries concerned should provide their consent. Due to the personal, sometimes intimate nature of beneficiaries' images and stories, and the potential long-term risks of such information being released into the public domain via print or the Internet, the procedure on informed explicit or implicit consent goes beyond the general guidance given above in Box 14.

The beneficiary should receive a clear explanation that:

- Once they release their consent, they will not be able to withdraw it
- They are under no obligation to agree to have their photo taken or share their information/story
- Refusing to have the photo taken or share their information or story will not result in any negative repercussions from the individual taking the photo/information or their agency. Conversely, consenting will not create any positive advantages (e.g. inclusion on beneficiary lists)
- They may opt to remain completely anonymous (e.g. by not giving their name, or by denying permission for their face to be shown or their voice to be recorded). In these cases a verbal agreement is sufficient.
- If they wish to remain anonymous:
    - The photographer or videographer shall produce the

photos or video in a way that they are not recognizable and show the final product to them;

- They are entitled to ask that any material that makes them feel uncomfortable be deleted.

Also:

- Wherever possible, materials using the image/information should be shown to the beneficiary
- No photo or video should be used without the specific and informed consent of the beneficiary.

Choices of images and messages will be made based on the following paramount principles of:

- Respecting the dignity of the people concerned.
- Representing any image or depicted situation both in its immediate and in its wider context so as to improve public understanding of the realities and complexities of the situation.
- Avoiding images and messages that potentially stereotype, sensationalize, stigmatize or discriminate against people, situations, or places (e.g. captioning photographs with information about their subject's HIV status or whether they have been raped).

Under no circumstances shall WFP personnel, cooperating partners, or contractors post photographs on any social media platform without the informed consent of beneficiaries.

Box 20
Key principles when using images of or stories about children

- Images of children should only be taken with parental permission (or with permission from the person legally authorized to give consent on behalf of the minor).

- The dignity and rights of every child are to be respected in every circumstance: images should only show children in a safe and dignified manner. For example, images of starving babies or of children wearing inappropriate clothing, or in any other demeaning situation, should be avoided.

- While interviewing and reporting on children, special attention is needed to ensure each child's right to privacy and confidentiality, to have their opinions heard, to participate in decisions affecting them, and to be protected from harm and retribution.

- The best interests of each child (see Box 15) are to be protected over any other consideration, including over advocacy for children's issues and the promotion of children's rights.

- When trying to determine the best interests of a child, the child's right to have their views taken into account are to be given due weight in accordance with their age and maturity.

- Those closest to the child's situation are to be consulted about the potential political, social and cultural ramifications of any reportage.

- The names and the visual identity of the following categories of children should be always changed and obscured:
  - victims of sexual abuse or exploitation;
  - perpetrators of physical or sexual abuse;
  - children who are HIV positive or living with AIDS;
  - children charged with or convicted of a crime;
  - child soldiers, or former child soldiers, who are holding a weapon or weapons.

In certain circumstances, when there is a risk or potential risk of harm or retribution, the names and the visual identity of the following categories of children should also be changed and obscured:

- former child soldiers who are not holding a weapon but may be at risk;
- asylum seekers, refugees or internally displaced persons.

As an ultimate criterion, stories or images that might put the child, siblings or peers at risk should be strictly avoided, even when identities are changed, obscured or not used. When there is any question or doubt, avoid using the images.

Refer to UNICEF's guidelines for further information:
http://www.unicef.org/media/media_tools_guidelines.html

Data Controller or Data Processor?

Depending on the situation, WFP may be considered to be the Data Controller; a Joint Data Controller; or a Data Processor. The following scenarios illustrate the differences in responsibilities between these roles.

Scenario 1: Data Controller

WFP is the Data Controller when it is the primary custodian of personal data and determines the purposes and manner in which personal data is processed. As Data Controller, WFP may delegate use of the data to other organizations or individuals, but it remains the ultimate responsible party for the protection of the data.

For example, WFP engages an NGO to register beneficiaries and collect their personal data on its behalf for a cash-based transfer intervention. WFP then provides this data to a Financial Services Provider to enable them to carry out their role in the intervention. In this case, WFP must respect the provisions of these Guidelines in all respects.

Scenario 2: Joint Data Controllers

When WFP engages with a third party to collect, store, and process beneficiary personal data for a joint specified purpose, both parties may be Data Controllers responsible for the data in their custody.

This shared role might arise, for example, when WFP is working in cooperation with other organizations, such as IOM or UNHCR, or when WFP acts as a service provider to another entity.

Another example is WFP executing social protection programmes on behalf of a government that is fully funding the programme and wants to retain equal custody and control of the beneficiary data.

This scenario is different from that of WFP as Data Processor (see Scenario

3) as WFP has end-to-end responsibility for execution of the programme. In such situations, WFP and their counterpart should negotiate their respective responsibilities prior to any data collection. WFP should endeavour to influence these negotiations in such a way that the provisions of these Guidelines are respected.

Scenario 3: Data Processor

WFP is the data processor when it does not have primary responsibility for the data collection, storage and processing. In this type of scenario, WFP typically receives data from a third party for a specified and legitimate purpose: for example, implementing an intervention.

For example, UNHCR provides refugee personal data to WFP to implement a food assistance programme. UNHCR remains the Data Controller, while WFP, as Data Processor, has responsibilities to protect the data under the terms of the FLA or DSA. (See Section 3 for more information on Inbound Data).

Retention and Disposal

WFP should *not hold personal data for longer than is necessary* to fulfil the specified legitimate purpose for which the data was collected. Afterwards, personal data should be either erased, returned or anonymized, according to WFP rules and what was agreed with the beneficiary or the originating party. The exception to this rule arises when an additional specified period is required for the benefit of beneficiaries.

This section is to be read in conjunction with Principle 2, which stipulates that WFP shall collect personal data only for specific, explicit and legitimate purposes. In the context of WFP's work, such purposes (e.g. implementing a specific project) have a finite duration. Unless an additional specified period is required for the benefit of beneficiaries (e.g. extending the length of a project), personal data that is no longer needed for fulfilling the purpose for which it was collected should either be destroyed or returned in compliance with WFP's Records Retention Policy.[21]

Anonymized data may be retained for WFP's legitimate organizational use, such as research and evaluation relating to WFP's mandate. However, caution should be exercised: data that is, on the face of it, ordinary, innocuous or without value may provide enough information to re-identify an individual — either by inference or through aggregation with data from other sources. Absolute anonymization of data sets can be complex, and much has been written on the subject. It is not within the scope of this document to provide comprehensive guidance on anonymization techniques, but information on the subject can be found via the links in the footnote below.[22]

---

[21] http://docustore.wfp.org/stellent/groups/public/documents/cd/wfp089773.pdf

[22] *Anonymisation: Managing Protection Risk* (2012) Information Commissioner's Office, UK. Online at: https://ico.org.uk/media/1061/anonymisation-code.pdf
Microdata Anonymization (web page) International Household Survey Network. Online at:

When records need to be disposed of, care must be taken to prevent any possibility of future retrieval. Paper records should be destroyed by burning. Electronic records should be destroyed with the advice and involvement of an IT Officer. Simply deleting records from a database or deleting files from the computer does not truly remove the data, so more sophisticated techniques need to be employed.

Contracts with third parties with which WFP intends to share beneficiary personal data should include clauses both on the period for which data may be retained and on deletion/return procedures.

Disposal records should be maintained and attached to project or evaluation reports. These records should indicate the date, time and method of destruction, as well as the nature of records destroyed.

http://www.ihsn.org/home/anonymization

4. Conducting a Privacy Impact Assessment (PIA)

A Privacy Impact Assessment is a project-based management tool in which risks to privacy are identified and assessed, and risk avoidance and/or mitigation strategies are developed. The PIA process shall be interwoven into the project cycle and should start at the Assessment and Risk Identification phase. In this way, WFP is embracing a "privacy by design" approach in which data protection and privacy risks are considered at an early stage of the project development.

Step 1. CO self-assessment

Each Country Office shall conduct an internal PIA to evaluate compliance with these Guidelines and determine what measures are in place to protect the confidentiality of beneficiary personal data.

Steps should be taken to ensure compliance with the Guidelines wherever possible, particularly those described under Principle 5: Security. Where full compliance is not possible, the CO should ensure that it understands what risk the organization, personnel, and beneficiaries are exposed to. This step need not be repeated each time a PIA is conducted for a new project, but should be revisited when changes occur that could have an impact on data protection and privacy — for example, relocation to a new office, or implementation of new information technologies.

Step 2.
Understand local legislation and regulations

Each Country Office shall understand the local legislative and regulatory requirements as they relate to data protection and privacy. As pointed out under Principle 1: Lawful and Fair Collection and Processing, WFP is not necessarily subject to domestic legislation. However, most, if not all, of its cooperating partners and service providers are bound by host countries' laws; therefore, it is important that WFP understands the conditions under which they must work.

Step 3.
Consult with the beneficiary community

Different segments of the beneficiary community should be consulted so that they can explain any concerns they have about the protection and privacy of their personal information. Any transfer modalities under consideration should be weighed as to which options beneficiaries would prefer or resist on the basis of the range and type of personal data required. Beneficiaries should also be consulted in order to jointly identify which mechanisms would be most convenient for them to request information about data processing, updating, modification, or erasure in a way that guarantees safety and confidentiality. Any considerations must take into account age, gender, ethnicity, and possible cultural, political and other vulnerability factors (see Box 21).

Step 4.
Describe the project

The description of the project should include some contextual information, such as: the size of the target population; budget; duration; planned modality; and what types of external partners will be involved (e.g. governments, NGOs, financial service providers, mobile telephone operators, market traders, etc.). The description should also include any relevant sociocultural consideration that may have an impact on project design or implementation.

Step 5.
Sectoral assessment of partners (macro assessments)

Each project planning cycle will necessarily involve sectoral assessments in which potential cooperating partners and service providers are evaluated. Operational risk identification surveys should include questions meant to assess the survey subject's data protection and privacy capacity and practices at a macro level. Sectors being assessed may include the following (with an indication of who would perform the assessment):

- Cooperating partners (Programme)
- Financial sector (Finance)
- Retail supply chain (Logistics and/or Procurement)
- Telecoms and IT sector (ICT)

Step 6.
Map data flows and identify vulnerability points

It is important to consult with all relevant stakeholders at an early stage of a project, so as to understand who needs which elements of personal data at what time, for which specific and legitimate purposes, and for how long. It may be useful to describe the information flows with particular attention to: who will collect what data from whom and for what specific purpose; how the information will be stored, secured, processed, and shared with others; and how this information will transferred. Any points in the data flows where potential vulnerabilities are exposed should be highlighted. To that end, use of data flow charts can be helpful.

Step 7.
Assess risk probability and impact severity (micro assessments)

In consultation with stakeholders, use the Risk Assessment Matrix below to identify and flag any potential vulnerability and assess whom these risks might impact, the probability of occurrence, and the magnitude of impact that an occurrence may have on data protection and privacy. Consider any local legislation or regulation when performing this assessment. Consider also the elements listed in Box 21.

Figure 1. Risk Assessment Matrix

Probability of occurrence	**Magnitude of impact**				
	1: Notable	2: Minor	3: Moderate	4: Major	5: Severe
5: Definite	Moderate	Significant	Significant	Extreme	Extreme
4: Likely	Moderate	Significant	Significant	Extreme	Extreme
3: Possible	Moderate	Moderate	Significant	Significant	Extreme
2: Unlikely	Low	Moderate	Significant	Significant	Extreme
1: Rare	Low	Low	Moderate	Moderate	Significant

Step 8.
Develop risk avoidance and/or mitigation strategies

Decide how to mitigate, eliminate, avoid, transfer, or accept the identified risks, in ways that are appropriate to their level of severity. If it is decided that certain risks are considered acceptable, document the justification. These strategies should be developed in close consultation with the party that will be responsible for implementing them.

Step 9.
Present report for approval

A report consolidating the findings from steps 1–8 of the PIA process should be presented to the Country Director for sign-off. The document should be retained throughout execution and referred to and reviewed when any identified or previously unforeseen risks are encountered in operations. A copy of the report should be forwarded to the DPO.

Box 21
Elements to consider in assessing risk probability and impact severity

- The nature, type, sensitivity, and intended and foreseeable use of personal data.

- Third parties, including foreseeable entities, with whom WFP intends to share personal data; whether they have data protection policies; and their capacity to ensure confidentiality and, more generally, compliance with WFP's data protection principles.

- Context: legislative, political, religious, ethnic and social contexts or other conditions that may interfere with data collection and processing.

- Special vulnerabilities, which may lead to culturally inappropriate situations, exclusion, harm, and/or biased information. In particular, three factors should be considered:

  - Age: disabilities, debility or particular social norms that may be attached to age may impede participation and/or full understanding by the people concerned.

  - Gender: household and community power dynamics, socially-ascribed roles, and the undue influence of husbands, fathers, family members and community leaders on women and young girls may lead to harm, discrimination, and self-censored and/or incorrect answers (or the reverse in matrilineal societies).

  - Other diversity characteristics: multiple factors such as language ability, illiteracy, disability, sexual life, political affiliation, ethnicity, and religious and cultural beliefs. All minorities, if they are subject to prejudice from the broader population, should be considered vulnerable to harm and exclusion.

- The degree of resistance from the beneficiary community that is likely to be experienced when considering the amount and nature of personal information that must be revealed in order for the planned modality to be implemented. A threshold of acceptable resistance levels should be set, and, if surpassed in the assessment, another type of modality should be considered instead. This should ensure that only a minimal portion of the beneficiary community will withhold or later withdraw consent for use of their personal data.

- The potential for fraudulent use of personal data.

- Potential risks to beneficiaries' safety and dignity.

- Anticipated benefits for beneficiaries, including positive spillover effects of the project/activity.

- Realistic mitigation measures that can be applied to contain the risk.

- When assessing a Financial Sector partner when a payment card modality is being considered, the institution's PCI DSS status should be evaluated (See Box 9).

While these Guidelines are not restricted to Cash Based Transfer (CBT) programmes, the diagrams below show how a PIA process could be integrated into a CBT project and offer an example that may be applied to other distribution modalities.

Figure 2. Integrating a PIA process with a CBT project cycle: overview

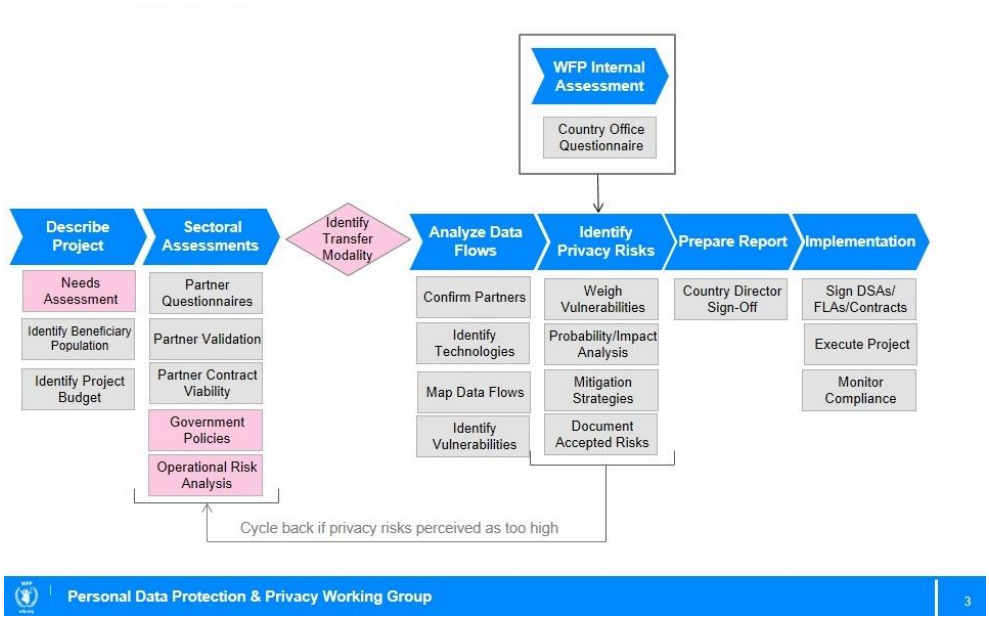
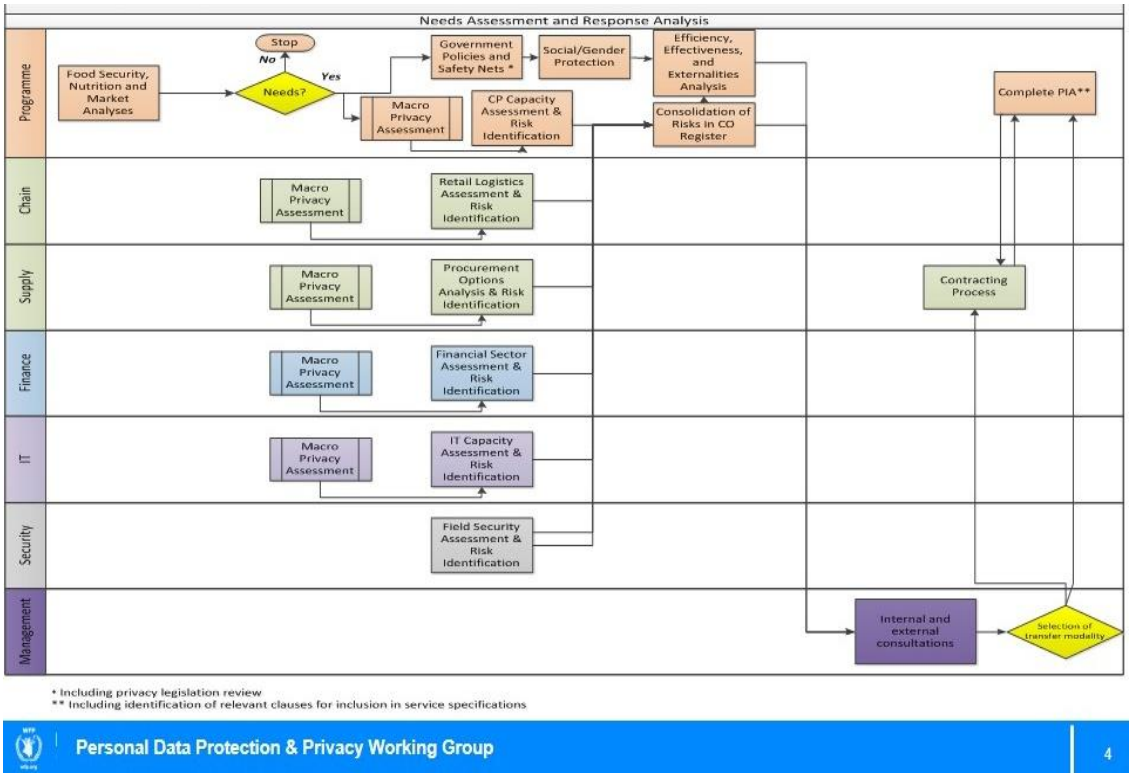


Figure 3. Integrating a PIA process with a CBT project cycle: summary, by division, of core responsibilities



5. Tools

Self-Assessment Compliance Checklist

The Country Office Data Protection Focal Point (DPFP), with the support of the Corporate Data Protection Officer, shall be responsible for checking that every concerned function/person mentioned below is in compliance with the present checklist.

Before collecting personal data		
What to check	**Reference in the Guidelines**	**Functions/person that may be involved**
Has a PIA assessment been conducted?	PIA, page 85	VAM, M&E, Procurement, Logistics, Programme, Field Monitors, IT, Security, Legal, cooperating partners and/or governmental partners involved
Have all factors that could expose beneficiaries to possible harm, and/or could bias fair and accurate data collection, been considered? (These factors include: gender-related customs and beliefs; political affiliation; ethnicity; religious and cultural beliefs; sexual life; age;	Lawful and fair collection and use, page 18 PIA, page 85	Programme, Field Monitors, cooperating partners involved and/or governmental partners involved

disability and debility; and language ability, etc. They also include potential fraudulence.)		
Has the risk of jeopardizing WFP personnel's security been addressed?	Lawful and fair collection and use, page 18 PIA, page 85	Programme, Field Monitors, Security, cooperating partners involved
Are privileges and immunities applicable in the host country?	Lawful and fair collection and processing, page 18	DCD, Head of VAM, Head of M&E, HoP with support from Legal
Is there any domestic legislation in the host country regarding privacy and personal data protection?	Lawful and fair collection and processing, page 18	DCD, Head of VAM, Head of M&E, HoP with support from Legal
Does domestic legislation contain any specific provision that is against international law? (If so, refer to legal to check how to proceed.)	Lawful and fair collection and processing, page 18	DCD, Head of VAM, Head of M&E, HoP. Legal to provide related advice
Does domestic legislation contain any provision that may force WFP's local partner to disclose personal data? (If so, risk of inappropriate disclosure needs to be assessed and taken into account.)	Lawful and fair collection and processing, page 18	DCD, Head of VAM, Head of M&E, HoP. Legal to provide related advice
Has the purpose of data collection been clearly identified and defined?	Specified and legitimate purpose, page 23	VAM, M&E, WFP's field monitors, enumerators, cooperating partners and governmental

		entities involved in data collection, private contractors
Have interviewers/enumerators been trained on how to collect personal data?	Lawful and fair collection and processing, page 18	Head of VAM, Head of M&E, HoP, cooperating partners and governmental entities involved in data collection, private contractors
Have beneficiaries been consulted on the degree to which they are comfortable with the data to be collected and with whom it will be shared?	Participation and accountability, page 28, PIA, page 82	WFP's field monitors, enumerators, cooperating partners and governmental entities involved in data processing, private contractors
Have beneficiaries been consulted with and their feedback incorporated in to the design of a mechanism to allow them to: • Receive information regarding anything that is related to handling, processing and protection of personal information; • Withdraw their consent; and • Correct or delete personal data	Participation and accountability, page 28, PIA, page 82	WFP's field monitors, enumerators, cooperating partners and governmental entities involved in data processing, private contractors
Have the mechanisms listed above been set up?	Participation and accountability, page 28	WFP's field monitors, cooperating partners and governmental entities involved in data processing, private contractors

Have all personnel and partners been trained on what to do in case of privacy breach?	Participation and accountability, page 28	CD, DCD, HR, IT
Are all personnel familiar with the content of these Guidelines?	Data security, page 37	CD, DCD, HR
Has a personal data focal point/officer been appointed?	Data security, page 37	CD, DCD
Have all the physical, technological and organizational measures — as set forth in the present Guidelines — been put in place?	Data security, page 37 Boxes 10, 11 and 12 on pages 41, 42 and 43	CD, DCD, IT, VAM, M&E, HoP, Administration, Facilities Management

At the time of collecting personal data		
What to check	**Reference in the Guidelines**	**Functions/people that may be involved**
Are beneficiaries being informed *at least* about: a) what type of personal data needs to be collected; b) the purpose for which it needs to be collected; c) who will access their data; and d) who they should contact, and how, if they have a concern regarding their data?	Specific application of the principles: Informed consent, page 46	WFP's field monitors, enumerators, cooperating partners and governmental entities involved in data collection, private contractors
Are beneficiaries releasing their consent? Is their consent explicit or implicit?	Specific application of the principles: Informed consent, page 46	WFP's field monitors, enumerators, cooperating partners and governmental entities involved in data collection, private contractors
In case of implicit consent, have the following, three conditions been fulfilled? a) The beneficiary has received all the information; b) There is no evident obstacle to the expression of his/her free will (e.g. linguistic or cultural barriers); and c) He/she has not put forward any objection after having been given the opportunity to do so.	Specific application of the principles: Informed consent, Box 13, page 49	WFP's field monitors, enumerators, cooperating partners and governmental entities involved in data collection

Is the interview location safe?	Lawful and fair collection and processing, page 18	WFP's field monitors, enumerators, cooperating partners and governmental entities involved in data collection, private contractors
Are all interviewed people capable, whether legally or in actuality, of providing their consent? (This concerns minors, people who may be incapacitated either cognitively or physically by disability or debility, and women [or men] who are not allowed to talk on behalf of the household.)	Specific application of the principles: Informed consent, page 46	WFP's field monitors, enumerators, cooperating partners and governmental entities involved in data collection, private contractors
If an interviewed person is not capable of providing their consent, can proxy consent be obtained from a parent/tutor/guardian, legal representative, or person with power of attorney of the person?	Specific application of the principles: Informed consent, page 46	WFP's field monitors, enumerators, cooperating partners and governmental entities involved in data collection, private contractors
If minors are interviewed, have interviewers received special training on how to interview children?	Specific application of the principles: Informed consent, page 46	Head of VAM, Head of M&E, HoP, cooperating partners and governmental entities involved in data collection, private contractors
Is the collected data of sufficient quality and quantity to meet the specified purposes or does it need to be improved or expanded through integration with other data?	Data quality, page 25	VAM, M&E, Programme, WFP's field monitors, enumerators, cooperating partners and governmental entities involved in

		data collection, private contractors
Is the collected data kept limited to what is necessary to fulfil the purpose? (Is all collected data actually being used?)	Data quality, page 25	VAM, M&E, Programme, WFP's field monitors, enumerators, cooperating partners and governmental entities involved in data collection, private contractors
Is information on ethnicity, political opinions, religious beliefs, health or sexual life, and/or biometric data being collected? If so, why? Is this data necessary to fulfil the specified purpose?	Data quality, page 25	VAM, M&E, Programme, WFP's field monitors, enumerators, cooperating partners and governmental entities involved in data collection, private contractors
Is protection-sensitive information being collected (e.g. enquiry about former combatant status, or whether the respondent has suffered any violence or coercion)? If so, why? Is this kind of information necessary to fulfil the specified purpose? Are interviewers trained to ask these kinds of questions?	Data quality, page 25 Lawful and fair collection and processing, page 18	VAM, M&E, Programme, WFP's field monitors, enumerators, cooperating partners and governmental entities involved in data collection, private contractors
Is the collected data detailed and truthful or does it need to be verified further and/or cross-checked?	Data quality, page 25	VAM, M&E, WFP's field monitors, enumerators, cooperating partners and governmental entities involved in data collection, private contractors

After collecting personal data **NOTE: Many of these elements MUST be in place BEFORE any data is collected, but would not be utilized until data has been collected.**		
What to check	**Reference in the Guidelines**	**Functions/people that may be involved**
Is electronically-stored personal data backed up on a regular basis?	Data security, page 41	IT
Are backup copies of personal data stored in a secure location that is different from the location in which the master data is stored?	Data security, page 41	IT
Are electronic transmissions of data encrypted?	Data security, page 42	IT
Is access to personal data restricted to only those whose job requires it?	Data security, page 42, 43	IT
Are different levels of access assigned to different individuals so that each person is restricted to accessing only the data they need to perform their job?	Data security, page 42, 43	IT
Are automated logs kept of who has accessed electronically stored personal data, for what action and when?	Data security, page 42	IT
Do systems force users to change passwords on a frequent basis?	Data security, page 42	IT
Do systems force users to create 'strong' passwords?	Data security, page 42	IT

If data is being used for a purpose other than the original one, does the other purpose have a reasonable and direct connection to the original one? Could it reasonably be expected that beneficiaries would consent to the other purpose, even if it was not spelled out at the time of consent?	Specified and legitimate purpose, page 23	VAM, M&E, Programme, cooperating partners and governmental entities involved in data processing, private contractors
In case of breach, are incidents reported to DPFP and/or Country Director?	Participation and Accountability, page 28	CD, DCD
Is data being destroyed after the specified purpose of collection and data processing has been fulfilled?	Specific application of the principles: Retention and disposal, page 80	VAM, M&E, HoP, IT
Is an IT officer involved in the destruction of electronic records?	Specific application of the principles: Retention and disposal, page 80	VAM, M&E, HoP, IT

Before receiving personal data from a third party		
What to check	**Reference in the Guidelines**	**Functions/people that may be involved**
Is a Field Level Agreement (FLA) or a Data Sharing Agreement (DSA) in place between WFP and the third party?	Specific application of the principles: Third-party data sharing, page 57	CD, DCD, VAM, M&E
Are the third party's procedures and policies complaint with WFP's principles?	Specific application of the principles: Third-party data sharing, page 59	VAM, M&E, HoP, IT, LEG
In particular, was data collected in a lawful and fair way by the third party?	Specific application of the principles: Third-party data sharing, page 59	VAM, M&E, HoP, LEG
Have beneficiaries provided their consent for their data to be shared with WFP (and other parties with whom WFP may further share)?	Specific application of the principles: Third-party data sharing, page 59	VAM, M&E, HoP
If no fully-informed consent was sought by the third party, has the third party or WFP obtained it at as soon as possible?	Specific application of the principles: Third-party data sharing, page 58	VAM, M&E, HoP
If not, is it reasonable to assume that beneficiaries would accept their data being shared with WFP and that using their data is in their best interest?	Specific application of the principles: Third-party data sharing, page 58	VAM, M&E, HoP

Is the data received limited to the minimum necessary?	Specific application of the principles: Third-party data sharing, page 58	VAM, M&E, HoP
Is data being destroyed after the specified purpose of collection and data processing has been fulfilled?	Specific application of the principles: Third-party data sharing, page 58	VAM, M&E, HoP

Before sharing personal data with a third party		
What to check	**Reference in the Guidelines**	**Functions/people that may be involved**
Is a Field Level Agreement (FLA) or a Data Sharing Agreement (DSA) in place between WFP and the third party?	Specific application of the principles – Third-party data sharing, page 57	CD, DCD, VAM, M&E, HoP
Do the FLA and DSA cover all key aspects of data sharing, as set forth by the present Guidelines?	Specific application of the principles: Third-party data sharing, page 65	CD, DCD, VAM, M&E, HoP
Have beneficiaries provided their consent for their data to be shared with third parties?	Specific application of the principles: Third-party data sharing, page 62	WFP's field monitors, enumerators, cooperating partners and governmental entities involved in data processing, private contractors
Were the formal and substantive conditions — as set forth in the present Guidelines — checked and confirmed as having been met before proceeding to data disclosure?	Specific application of the principles: Third-party data sharing, page 62 62	VAM, M&E, HoP
Are the third party's procedures and policies complaint with WFP's principles?	Specific application of the principles: Third-party data sharing, page 62	VAM, M&E, HoP, LEG, IT, Procurement, Logistics

In particular, is the third party able to ensure the same security measures as set forth in the present Guidelines?	Specific application of the principles: Third-party data sharing, page 62	VAM, M&E, HoP, LEG, IT, Procurement, Logistics
Are Financial Service Providers (when used for a card-based intervention) compliant with Payment Card Industry Data Security Standards?	Specific application of the principles: Data Security, page 39	Procurement
If children were involved in data collection and the use of image and stories: were the special conditions — as set forth by the present Guidelines — checked and confirmed as having been met?	Specific application of the principles: Informed Consent, page 54 and Media, page 78	HoP, COM

Minimum Standards for Exceptional Circumstances

These Guidelines provide a comprehensive set of operational standards for personal data collection and processing in WFP's operations. WFP shall comply with it to the best of its ability and whenever the situation allows it. However, there may be cases (e.g. sudden-onset crises or a massive influx of refugees) where the nature of the operation does not allow compliance with all the Guidelines' provisions. The following checklist is meant to highlight the minimum requirements that should be met in all circumstances, regardless of the urgency and gravity of the situation.

Before collecting data

- Be clear about which personal data is actually needed and the specific purpose for which the data needs to be collected. Prepare questions accordingly so as to avoid requesting unnecessary information.

- Check whether the data collection plan will require beneficiaries to provide information about their ethnicity, political opinions, religious beliefs, health or sexual life, and whether it will involve the recording of biometric data. If so, make sure that these types of data are absolutely necessary to the specified purpose. If not, do not collect them.

- Check whether the plan for data collection includes questions related to protection-sensitive information (e.g. asking beneficiaries about former combatant status or security incidents, etc.). If so, make sure that this type of information is necessary to the specified purpose and that interviewers are trained to ask these questions. If the information is not necessary, or interviewers do not have the right training, do no collect this type of data.

- Analyse all factors that may expose beneficiaries to possible harm as a result of personal data collection and the use of that data. These factors include: gender-related customs and beliefs, political affiliation, ethnicity, religious and cultural beliefs, sexual life and age, as well as possible fraudulent use of the data should a breach occur. Take mitigation measures, as necessary.

- Bearing in mind the local security situation, analyse all possible risks to WFP personnel that might arise from the collection and use of personal data. Take mitigation measures, as necessary.

When collecting data

- Inform beneficiaries on:
  - what type of personal data needs to be collected;
  - the purpose for which personal data must be collected;
  - who will access their data; and
  - who they can contact if they have a concern about their data.
- Obtain explicit or implicit consent from the beneficiaries (see Section 3, Informed Consent).

After collecting data

- Make sure that data is stored in a safe and secure environment (either physical or virtual) to which access is limited to authorized people only
- Make sure data is destroyed (or, in the case of inbound data, returned to the third party) once the specified purpose is met.

When receiving or disclosing data from or to third parties

- WFP should make sure that beneficiaries have provided their consent for:
  - their data to be shared with WFP/the third party; and
  - the intended use of their data.

- If receiving third party data for which no consent was obtained:
  - WFP should ask the third party to obtain consent.
  - If that is not possible, WFP should attempt to obtain it directly from beneficiaries.
  - As a last resort, WFP must judge whether beneficiaries could reasonably be expected to accept the sharing of their data with WFP (inbound), or with the third party (outbound). WFP must also judge whether using the data is in the beneficiaries' best interest. If WFP concludes that the answer is 'yes' in both cases, proceed with the use of this data.
- WFP should have a specific data sharing agreement in place with the third party. Ideally, this should be set up before the disclosure takes place; if not, then as soon as possible afterwards. Draft agreements should be referred to LEG for advice. Clauses should be included to cover the following points:
  a) the type of personal data needed;
  b) the specified legitimate purpose;
  c) depending on the situation, either the prohibition of use for previously unforeseen purposes and disclosure to other parties, or conditions for further use and disclosure;
  d) the retention period;
  e) the method of destruction, return or anonymization; and
  f) procedures to follow in the event of a breach.
- When sharing data with a third party add a note for the file to the personal data records. The note will indicate: the date of disclosure; the type of information disclosed; to whom it has been disclosed; and the specified purpose for use of the data.

Model Consent Forms

Templates for WFP data protection notice and beneficiary consent form, data access request form, and photo/video release form

The form templates in this Section should be used and filled in by WFP personnel or by implementing partner/service provider personnel authorized to collect beneficiary data on behalf of WFP. Instructions for completing a form are printed in *italic*.

The templates provided are as follows:

Form A. Notice and Consent Form for collection of beneficiary personal data.

Form B. Data Access Request Form for beneficiaries seeking access to their personal data.

Form C. Communications Subject Release Form (for photos and videos).

Form A

Notice and Consent Form for collection of beneficiary personal data by, or on behalf of, the World Food Programme (WFP)

Date and place of data collection: _____

Details of the person filling in this form and seeking the respondent's consent:

- Name: _____
- Title: _____
- The person's organization: _____
- The organization for which the data is being collected: _____
- Language in which information is provided: _____

If applicable:

- Name of the interpreter or translator: _____
- The interpreter's or translator's relationship with the beneficiary: _____

Type of personal data of the individual concerned for which consent is given:

First and middle name:	☐	Surname:	☐
Identification or registration number:	☐	Place of birth:	☐
Marital status:	☐	Date of birth/age group:	☐
Gender:	☐	Mobile phone number:	☐
Address:	☐	Biometrics (fingerprints and/or other):	☐
Other data [please specify below]:	☐		

_____

If consent is not given for any option, please indicate reasons why (if possible):

_____

Purposes of collection

WFP, and any authorized person or entity acting on behalf of WFP, may only collect and use my personal data for the following purposes.

Original specified purposes:

- Eligibility to be included in the Programme: ☐
- Continuous assistance: ☐
- Provision of assistance: ☐
- Monitoring and evaluation of the Programme: ☐
- Other purposes *[please specify below]*: ☐

Additional foreseeable purposes *[please specify]*: ☐

If consent is not given for one or more of the specified purpose/s, please indicate reasons why (if possible): _____

Transfer of personal data

I am aware and I agree that in order to fulfil the purposes as set out above WFP may share my personal data with third parties including:

Other UN agencies:	☐	Implementing partners:	☐
WFP service providers (e.g. banks, card issuers):	☐	Local/government authorities:	☐
Other *[please specify below]*:	☐		

If consent is not given for data to be shared with one or more of the specified third party/ies, please indicate reasons why (if possible): _____

The respondent's right to access, amend and delete their personal data

I understand that I may request access to, modifications to, and/or deletion of my personal data, or submit any queries about my personal data by *[Please select and include applicable method/s]**:***

- Contacting WFP at *[insert email address]*: ☐

- Completing the attached Data Access Request Form and returning it to WFP: ☐

Release of liability and claims

I hereby release WFP, its licensees and assignees, from all liability and claims of any nature whatsoever resulting from or connected with the use of my personal data in accordance with this Form.

Data security

I understand that WFP has security measures in place and will use its best endeavours to protect my personal data from unauthorized use, and to ensure that only duly authorized individuals will be able to access my personal data for the abovementioned purposes.

I understand that I should inform WFP if I believe that an unauthorized individual has accessed my personal data.

Declaration by respondent

I declare that I have understood the content of this form *[please tick relevant box]*:

- After having read the above clauses: ☐

- After having the above clauses read and/or translated to me: ☐

I declare that the information I have provided is true and correct to the best of my knowledge. I voluntarily make this declaration and freely consent to the collection and processing by WFP and any authorized persons or entity acting on behalf of WFP of my personal data, and, if applicable, that of my dependants.

Form of consent

i. The name of the beneficiary *[please write this in capitals]*:

_____

ii. Consent is given by *[please tick relevant box]*: the beneficiary ☐

by their proxy ☐

other ☐

iii. Signature of the beneficiary/proxy: _____

iv. Fingerprint of the beneficiary/proxy: ☐

v. The beneficiary's/proxy's mark: _____

vi. Proxy consent

Name of the person giving proxy consent, and in what capacity:

_____

vii. Other means of obtaining consent and reasons for this:

_____

_____

Form B

Data Access Request Form

Please complete this form if you wish to access, modify, and/or delete personal data belonging to you and/or, where applicable, your dependants, held by the World Food Programme (WFP). Following receipt of this completed form, WFP will inform you whether the organization needs more information in order to address your request or concern.

First and middle name:

_____

Surname:

_____

Date of birth/age group:

_____

Identification or registration number:

_____

Telephone number:

_____

Email:

_____

Address:

_____

Are you *[please tick relevant box]*:

The data subject	☐
A parent/guardian of the data subject	☐
A representative of the data subject with legal authority	☐

Please specify your request:

Access ☐ Modify ☐ Delete ☐

Please provide as much detail as possible about your request:

_____

_____

_____

Date and Place: _____

Signature of the beneficiary: _____

Fingerprint of the beneficiary: ☐

Please return this form to WFP *[insert mailing/email address]*.

_____

OR

Returned by hand to WFP representative:

Date and place: _____

_____

Name of WFP representative: _____

_____

Title of WFP representative: _____

_____

Form C

Communications Subject Release Form

Name: _____

Date: _____

Address/location: _____

Release

I, being of legal age and capacity, hereby give my irrevocable consent in perpetuity to the World Food Programme to: (i) take photographs of me and record my voice, image, appearance and performances; and (ii) edit, duplicate and use, or license others to edit, duplicate and use, the same (and my name), separately or in conjunction with other works, content or materials, worldwide and in any media or manner, for the purpose of raising awareness of and funds for the World Food Programme, and its fight against hunger.

I understand that there will be no financial or other remuneration for any such use of my name, picture, image, appearance or performances and hereby release the World Food Programme, its licensees and assigns, from all liability and claims of any nature whatsoever resulting from or connected with the use thereof.

Signature[23]: _____

If the subject is a minor:

Name of minor (in block letters):

_____

I, being of legal age and capacity, have legal custody of the minor named above, have

[23] If the subject wishes to make a mark or fingerprint (rather than sign), please note next to it 'the mark/fingerprint of [initials]'

read this release and hereby consent to all of its terms. I represent and warrant that the minor named above will not disavow this consent on the grounds that s/he was a minor at the time of signature or on any other grounds whatsoever.

Print name: _____

Signature:

The person asking the subject or his/her parent/guardian to sign this release form should read the following statements to them to ensure that the person fully understands what they are about to sign.

“By signing this form you authorize WFP to:

- Take video and/or still photographs of you and record your voice;
- Freely share these videos, photographs and recordings with other people and institutions worldwide (who, in turn, might use and share with other people);
- Use these photographs and recordings in media (TV, radio, printed publications, social networks or other internet platforms such as WFP’s web pages or video streaming services).

All the above will be done with the purpose of raising awareness of and funds for the World Food Programme, and its fight against hunger.
You further understand that there will be no money or other compensation given to you by WFP or anyone with whom WFP shares these videos, photographs, and recordings, and that once given this consent cannot be revoked at any time, or for any reason.”

If the subject is a minor, read the above section (amending it to refer to the minor) and then read the following:
“You confirm that you are of legal age and capacity and have authority to provide this consent on behalf of the minor.

You have understood the content of this form as explained above and agree to its terms.

You understand that by signing this release the minor that you represent will not have any recourse to revoke this consent at any time, or for any reason, including for the reason that he/she was a minor at the time that you signed the form on his/her behalf."

6. Acronyms

ATM	Automated or automatic teller machine
CBT	Cash Based Transfer
CD	WFP Country Director
CO	WFP Country Office
COM	Communications Division (WFP HQ)
DCD	WFP Deputy Country Director
DPFP	CO Data Protection Focal Point
DPO	HQ Data Protection Officer
DSA	Data Sharing Agreement
EMOP	emergency operation
FFA	Food Assistance for Assets
FLA	Field Level Agreement
FSP	Financial Services Provider
HIV	Human Immunodeficiency Virus
HoP	Head of Programme
HQ	WFP Headquarters

HR	Human Resources Division (WFP HQ)
IASC	Inter-Agency Standing Committee
ICC	International Criminal Court
ICT	Information Technology Division (RMT) (WFP HQ)
IOM	International Organization for Migration
ID	Identification
IDP	Internally displaced person
IOM	International Organization for Migration
IREMOP	Immediate Response Emergency Operation under CO authority
KYC	Know Your Customer
IT	Information Technology
LEG	Legal Office (WFP HQ)
M&E	monitoring and evaluation
MoU	memorandum of understanding
NGO	non-governmental organization
OSZ	Policy and Programme Division (WFP HQ)
PCI DSS	Payment Card Industry — Data Security Standard
PIA	Privacy Impact Assessment
POS	Point of Sale
SCOPE	WFP's IT system for beneficiary management

SIM	Subscriber Identification Module (card in mobile phone)
SMS	Short Message Service
TV	television
UN	United Nations
UNHCR	United Nations High Commissioner for Refugees
UNICEF	United Nations Children's Fund
VAM	vulnerability assessment and mapping
WFP	World Food Programme