Journey of a beneficiary: towards a digital transformation to better support those we serve

Update to the Executive Board

30 October 2018, 14:00 – 15:30

WFP Headquarters

Concept Note : WFP's Data Privacy and Protection Framework

Background

We are currently living in the era of "data revolution." Advances in information communication technology are dramatically increasing the volume, types and speed of available data, creating unprecedented possibilities for informing and transforming the society, enforcing people's rights, improving the way people in need access assistance. There is a unanimous recognition that data will play a key role in monitoring progress on SDGs, holding governments accountable and fostering sustainable development. WFP's business models are rapidly evolving with it, as its operations are increasingly informed by and/or built upon state-of-the art technological innovations such as WFP's Digital identity management solution SCOPE and Electronic solutions in Cash-Based transfer (CBT) programming (e.g. mobile banking, electronic vouchers, SCOPE cards).

WFP assists over 90 million people in around 80 countries each year. WFP is the leading humanitarian organization saving lives and changing lives. This means processing a large amount of data and information, including the personal data of its beneficiaries and prospective beneficiaries. Currently, 31,207,366 people we serve are registered in SCOPE in 59 countries. As of October, a total of $1.3 billion has been transferred in 2018, to assist over 12.9 million beneficiaries through Cash-based Transfers (CBT). In 2017, WFP transferred $1.4 billion through CBT, assisting a total of 19.2 million beneficiaries.

The purpose of this background note is to provide an overview of WFP's existing data governance frameworks, and the strategies either in place or being put in place to ensure we have the highest level of data safeguarding and security for the critical data that it holds. Protecting the data of those we serve is a fundamental part of WFP's chief accountability.

Information Systems and Data Governance Framework

The Management Information Systems Steering Committee (MISSC) chaired by the Deputy Executive Director is responsible for setting the strategic direction of WFP's information technology investments. The MISSC reviews the TEC strategic plan, provides advice to the Executive Director on enterprise and IT architectures, including information architecture covering assignment of information, applications and critical transaction ownership. The MISSC also reviews and obtains organizational acceptance of business risks of IT, oversees security of WFP's critical systems, and defines a "value for money" approach for organization-wide tracking of tangible and intangible benefits arising from IT-enabled projects. A board of external advisors, the IT Advisory Board (ITAB), has been established to support the MISSC function in continuously reviewing the IT Strategy and advising the MISSC accordingly in light of leading industry themes and management practices in IT.

A Data Governance Framework was established in 2014 on the basis of an ED Circular (OED 2014/005 WFP Master Data Governance Framework) to establish the framework for enterprise master data management, enhance the role of the MISSC as the Data Governance Board and identify the roles and responsibilities of key data owners and stewards. The governance structure is composed of the data governance authorities, data governance policies, data and information. Data and information are stored in WFP applications, the Enterprise Data Warehouse and the Master Data Repository.

In the context of defining and maintaining responsibilities for ownership of information (data) and information systems, the MISSC established the Data Management Committee (DMC) in August 2017 to operationalize the direction and priorities set by the Data Governance Board, implementing good data management practices and recommending the strategy for all data including master data, meta data, big data, open data, and for the management of privacy, security and ethical use of data. Its objective is to improve the quality of information, based on trusted data, for evidence-based decision-making in operations and financial management.

The Chief Information Officer and Director of the Technology Division provides guidance on data management best-practice to Data Owners and Stewards. Data Owners are accountable and responsible for ensuring the correctness of the information associated to their Data domain throughout their activities and for controlling the content and the exchange of information within the official repositories of data and other business applications. The Data Owner manages access rights to data, and nominates Data Stewards to assure consistency, completeness and currency of data in applications.

Key Information Systems

The enterprise information systems landscape of WFP is composed of four corporate applications – WFP Information Network and Global Systems (WINGS), Logistics Execution Support System (LESS), Country Office Tool for Managing Effectively (COMET) and SCOPE – that are enabled by the data analytics foundation which includes an enterprise data warehouse and a data lake – a corporate storage repository that holds vast amount of raw data.

WINGS is the information system used to manage many facets of WFP's business, including programme/project planning and implementation, procurement, supply chain, finance, travel and human resources. LESS provides business management support for WFP's commodity supply chain process. It is a tool for tracking commodities enabling our optimization of food resources by managing our supply chain enhancing our visibility, accuracy and cost-efficiency. COMET is WFP's Country Office Tool for Managing Effectively, supporting programme management to design, implement and monitor WFP programmes and improving organizational performance. SCOPE is WFP's beneficiary and transfer management system that informs on who the beneficiaries are, what they are entitled to, issues instructions to the appropriate delivery mechanism and receives feedback whether the transfer was received or not by the beneficiary.

Personal Data Protection at WFP

For WFP to serve people rapidly and efficiently with our assistance services, WFP needs to identify its beneficiaries. WFP is rapidly advancing our path of digitalization and this has resulted in increasing amounts of beneficiary personal data being acquired by WFP and stored in its information systems. This has provided opportunities for greater programme effectiveness and operational efficiencies, and enabled WFP to scale-up humanitarian action using cash-based modalities. In today's fast-changing digital world, we are working diligently and deliberately to find ways to maximize benefits and minimize risks to holding this data. We are taking steps to strengthen our own technical systems.

WFP has become increasingly aware of the data protection issues inherent to the use of technological innovations. In response to these concerns, in January 2017, WFP issued the Guide to Privacy and Personal Data Protection. The Guide sets forth five standards, which represent the backbone of WFP's approach to personal data protection and address the main problems that relate to the entire data processing cycle, from collection to destruction. The standards are meant to be used across the whole spectrum of WFP's activities involving technologies, notably SCOPE, mVAM, cloud computing, use of drones, biometrics, big data analysis, cash-based programs. It covers the 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. The individual's right to privacy is enshrined in various international legal instruments and principles, include the Universal Declaration of Human Rights. WFP needs to respect the right to privacy and the protection of personal data.

With the publication of WFP's Guide to PDPP, WFP also began operationalizing the PDPP. A number of steps have already been taken and several others are in development, as noted below:

- In order to better enhance the data protection and privacy posture of the organization and define accountability, an ad interim Data Protection Officer was put in place in Programme to govern beneficiary data, and a Data Protection Officer for information security was put in place in the technology division. An enterprise-level data protection framework and structure for all types of data is being finalized before the end of the year, an essential first step before planning and implementing policies
- "Conducting Mobile Surveys Responsibly: A Field Book for WFP Staff" was issued May 2017. It outlines the main risks for staff engaged in mobile data collection and helps promote responsible data collection/storage/sharing in the very complex environment in which WFP operates.
- "WFP Data Week" is a new and planned to be annual occasion for socializing and mainstreaming data literacy, data security, integration and overall good data practices across the organization. A class of Data Fellows from diverse divisions and country offices serve as internal expert ambassadors throughout the year.
- A data lake is being built to address data accessibility challenges around the organization. The data lake sources data from five corporate systems (Budget & Planning Tool, COMET, MDCA, Salesforce, and WINGS), breaking down silos between data sources and allowing dashboards to pull from the same data sources. This will enable analytics, reporting, and beyond to be able to be generated with the most up-to-date data available.
- WFP has had beneficiary data stored in its central systems since 2014. A beneficiary personal data lifecycle standard is being finalised to define the policy by which personal data is managed, archived, and eventually, removed from WFP records when no longer used.
- The personal data collected at WFP goes beyond that of beneficiaries (for example, staff data is collected and processed by many divisions). Because personal data collection is so diffuse, the DMC is discussing and defining the role of the future Data Protection Officer, including where it makes most sense for that role to fit within the organization. This decision will be based on what data is being processed by which divisions, the other WFP policies and measures currently in place, and best practices from other organizations (both peer humanitarian and international).

WFP and data protection externally – Data Sharing and Partner Considerations

We are working with partners to refine policies and practices as new challenges are understood. For example, we are among several UN agencies and NGOs that have been working to clarify and establish guidelines and best practices in the area of responsible data use.

WFP is a member of groups like the Global Partnership on Sustainable Development Data, the International Data Responsibility Group, and the Centre for Humanitarian Data that are all fora for exchanging and learning best practices about data innovation and use.

The UN Development Group recently endorsed a set of guidelines on data privacy ethics and protection related to Big Data. UNDG is an inter-agency group and WFP was party to the committee that developed and drafted the guidance note.

WFP undersigned the UN Personal Data Protection and Privacy Principles as agreed on by the UN System Organization Representatives on 12 October 2018.

Data sharing agreements have been finalized at CO levels with several organizations, such as International Organization for Migration (IOM), United Nations International Children's Emergency Fund (UNICEF) and United Nations High Commissioner for Refugees (UNHCR). A global data sharing agreement has been signed with UNHCR to share where appropriate beneficiary information, among others. WFP does not share or provide access to beneficiary information unless underpinned by a data sharing agreement with an agency that adheres to the same data protection principles to which WFP adheres. When data sharing occurs, SCOPE is able to import in bulk the registries of other agencies, and is seeking to create inter-operable solutions with other parties to automate the entire process.

IT Security and Safeguarding of Beneficiary Personal Data

Constant work is being done to improve our systems and ensure there is no breach, and no data leakage. WFP has put in place a multi-functional set of actions to further improve the security posture for safeguarding this data.

At the technical level, WFP continually commissions security penetration tests on WFP's technical infrastructure as well as key applications such as SCOPE, including those performed by external security companies. Threat and risk assessments have been performed by external parties, and an application audit has been performed by WFP's internal auditors.

The business controls are enforced by application controls established in technical solutions such as SCOPE. These controls have been designed to respect segregation of duty rules (SoD) as well as corporate process standards such as the CBT Business Process Model (BPM).

A secure password mechanism is in place to control access to both online and offline applications. These accounts are regularly checked for activity and disabled when no longer used, with access provided following the principle of least privilege. Multi-factor access control mechanisms are planned to be implemented by year end to further strengthen access security.

Sensitive data are encrypted upon collection in the field, during transmission, and during storage at central facilities. Data on WFP's smartcards that are distributed to beneficiaries are encrypted with hardware-supported encryption mechanisms. When using SCOPE, no personal data is kept in field offices, as all sensitive data is stored and secured at WFP's data centres, and backed up in secure UN facilities.

Activities are in progress to assess the cyber-security maturity of WFP's financial service providers and, where applicable, determine the level of protection that these vendors provide to beneficiary data that they hold.