Information Privacy

United Nations Children's Fund

Prepared For: Internal Stakeholders and United Nations Oversight Bodies

Group E

Travis McGhee, Ali Aita, Ethan Payne, Anthony Hastaba

1. Introduction

1.1 Overview The United Nations Children's Fund (UNICEF) operates in over 190 countries and territories to save children’s lives, to defend their rights, and to help them fulfill their potential. In the pursuit of this mandate, UNICEF is required to collect, process, and utilize specific Personally Identifiable Information (PII) regarding our staff, donors, partners, and beneficiaries. This policy formally declares that the organization recognizes the critical value of this data and dictates strict protocols on how such PII is to be protected to ensure safety, dignity, and trust.

1.2 Purpose This document serves as the comprehensive governance framework for information privacy at UNICEF. It establishes the standards for data handling from the moment of collection through to archiving or destruction. By adhering to this policy, UNICEF ensures that it operates within the bounds of ethical data management while maintaining the transparency required by our stakeholders.

1.3 Definitions and Terminology To ensure clarity and consistent interpretation of this policy across all UNICEF offices globally, the following terms are defined as follows:

- **Personally Identifiable Information (PII):** Any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

- **Sensitive PII (SPII):** A subset of PII that requires higher levels of protection due to the risk of significant harm to the individual if compromised. For UNICEF, this includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.
- **Data Subject:** The individual to whom the PII refers. In the context of UNICEF operations, data subjects primarily include beneficiaries (children and families receiving aid), donors (individuals contributing financial support), employees, consultants, and volunteers.
- **Data Controller:** The entity that determines the purposes and means of the processing of personal data. For the purposes of this policy, UNICEF Headquarters is the primary Data Controller.
- **Data Processor:** An entity that processes personal data on behalf of the Data Controller. This includes third-party vendors, cloud service providers (e.g., Microsoft Azure, AWS), and implementing partners (local NGOs) who handle UNICEF data.
- **Consent:** Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.
- **Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

- **Pseudonymization:** The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- **Encryption:** The process of converting information or data into a code, especially to prevent unauthorized access. UNICEF mandates AES-256 encryption standards for all SPII at rest.

2. Rationale for Policy

2.1 Necessity of Compliance This policy is required to ensure UNICEF remains in compliance with a complex web of international regulations and laws. As a global entity, we must navigate the legal requirements of the countries in which we operate while maintaining the privileges and immunities of the United Nations.

2.2 Protection of Rights The primary rationale for this policy is the protection of rights. We are ethically and legally bound to protect the rights of our staff, our valued customers (donors), and our business partners. Most critically, we must protect the privacy of the children and families we serve. For vulnerable populations, a privacy violation is not just a digital inconvenience; it can pose life-threatening risks, including stigmatization, persecution, or physical harm.

2.3 Risk Mitigation This policy is designed to protect the organization against the severe risks associated with privacy violations. These risks include legal liability, financial loss, and catastrophic reputational damage. By enforcing this policy, UNICEF aims to prevent breaches of

confidentiality that could undermine public trust and jeopardize our ability to deliver aid to those in need.

3. Laws and Regulations

UNICEF's data operations are guided by the following pertinent laws and regulations:

- **General Data Protection Regulation (GDPR):** While UNICEF operates under UN immunity, we align our data practices with the GDPR to ensure the highest standard of protection for donors and staff located within the European Union. This includes respecting rights to data access, rectification, and the "right to be forgotten."
- **The U.S. Privacy Act of 1974:** As we maintain significant operations and fundraising activities within the United States, we adhere to the principles of the U.S. Privacy Act regarding the collection and use of data belonging to U.S. citizens and permanent residents.
- **UN Principles on Personal Data Protection and Privacy:** This internal UN framework provides the overarching guidelines for all UN agencies, ensuring a harmonized approach to data privacy across the UN system.
- **Convention on the Rights of the Child (CRC):** Specifically, Article 16, which mandates that no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, or correspondence.

4. Fair Information Practice Principles (FIPPs)

This policy is implemented under the guidance of the Fair Information Practice Principles (FIPPs), which serve as the foundation for privacy law globally.

- **Principle of Transparency:** UNICEF must be open about its data practices. Individuals should have clear knowledge of what data is being collected and how it will be used.
- **Principle of Individual Participation:** Individuals should have the right to access the data held about them and to contest its accuracy or completeness.
- **Principle of Purpose Specification:** The purpose for which personal data is collected should be specified not later than at the time of data collection. The subsequent use of the data is limited to the fulfillment of those purposes.
- **Principle of Data Minimization:** The collection of personal data should be limited to that which is relevant and necessary for the identified purposes.
- **Principle of Use Limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.
- **Principle of Security Safeguards:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.
- **Principle of Accountability:** UNICEF is accountable for complying with measures which give effect to the principles stated above.

5. Policy Scope

5.1 Organizational Scope This policy applies to the entire UNICEF ecosystem. This includes the main headquarters in New York, all regional and country branches, all research centers (Innocenti), and supply divisions.

5.2 Personnel Scope Compliance is mandatory for all personnel, regardless of contract type. This includes all full-time employees, part-time staff, interns, volunteers, and all contractors and suppliers who have access to UNICEF data systems.

5.3 Data Scope This policy protects all data considered to be Personally Identifiable Information (PII). This encompasses:

- **Basic Identifiers:** Names, physical addresses, email addresses, and phone numbers.
- **Sensitive Identifiers:** Social Security numbers (or national ID equivalents), passport details, and financial account numbers.
- **Beneficiary Data:** Biometric data (fingerprints/iris scans used in aid distribution), medical history, and geolocated case files.

6. Data Protection Risks

6.1 Overview of Risk Landscape UNICEF operates in some of the most volatile and complex environments in the world. As such, the risks associated with data privacy are not merely technical inconveniences; they are operational threats that can endanger lives. We face a diverse array of privacy risks that require constant vigilance, assessment, and mitigation.

6.2 Key Privacy Risks The organization has identified the following primary categories of risk regarding the processing of PII:

- **Breaches of Confidentiality:** This is the most critical risk facing our beneficiary data. A breach of confidentiality occurs when sensitive PII (such as the location of a shelter, the HIV status of a child, or the political affiliation of a local partner) is disclosed to unauthorized entities. In conflict zones, such a breach could result in the physical targeting, kidnapping, or persecution of the individuals we serve.
- **Failure to Offer Choice:** There is a significant risk that, in the rush to deliver emergency aid, data subjects (beneficiaries) are not given a genuine choice regarding their data. If UNICEF collects data without obtaining informed consent or without offering an "opt-out" mechanism, we violate the dignity of the individual. This risk is particularly acute when working with illiterate populations or children who cannot legally consent.
- **Reputational Damage:** UNICEF relies entirely on voluntary contributions from governments and private donors. A significant privacy failure—such as a leak of donor credit card information or a scandal involving the misuse of children's data—would cause catastrophic reputational damage. This loss of trust would directly translate into a loss of funding, crippling our ability to save lives.
- **Data Integrity and Accuracy Risks:** If PII is not kept accurate, it poses a risk to aid delivery. For example, if a medical record for a child is incorrect due to data entry errors, that child may receive the wrong vaccination or be denied necessary food rations.
- **Third-Party Transfer Risks:** UNICEF frequently partners with local NGOs and commercial vendors to implement programs. There is an inherent risk that these third parties may not adhere to the same high standards of privacy as UNICEF. Without strict contractual clauses and monitoring, data shared with partners effectively leaves our control.

7. Responsibilities

7.1 Governance Structure To effectively manage the risks outlined above, UNICEF has established a clear chain of command and responsibility regarding data privacy. Privacy is not solely the domain of the IT department; it is a shared responsibility across the entire organization.

Here is **Part 2** of the text. This section is designed to be text-heavy to help you reach your page count.

Formatting Reminder:

- Insert a **Page Break** before the header "**6. Data Protection Risks**."
- Insert a **Page Break** before the header "**7. Responsibilities**."

---

6. Data Protection Risks

6.1 Overview of Risk Landscape UNICEF operates in some of the most volatile and complex environments in the world. As such, the risks associated with data privacy are not merely technical inconveniences; they are operational threats that can endanger lives. We face a diverse array of privacy risks that require constant vigilance, assessment, and mitigation.

6.2 Key Privacy Risks The organization has identified the following primary categories of risk regarding the processing of PII:

- **Breaches of Confidentiality:** This is the most critical risk facing our beneficiary data. A breach of confidentiality occurs when sensitive PII (such as the location of a shelter, the HIV status of a child, or the political affiliation of a local partner) is disclosed to unauthorized entities. In conflict zones, such a breach could result in the physical targeting, kidnapping, or persecution of the individuals we serve.
- **Failure to Offer Choice:** There is a significant risk that, in the rush to deliver emergency aid, data subjects (beneficiaries) are not given a genuine choice regarding their data. If UNICEF collects data without obtaining informed consent or without offering an "opt-out" mechanism, we violate the dignity of the individual. This risk is particularly acute when working with illiterate populations or children who cannot legally consent.
- **Reputational Damage:** UNICEF relies entirely on voluntary contributions from governments and private donors. A significant privacy failure—such as a leak of donor credit card information or a scandal involving the misuse of children's data—would cause catastrophic reputational damage. This loss of trust would directly translate into a loss of funding, crippling our ability to save lives.
- **Data Integrity and Accuracy Risks:** If PII is not kept accurate, it poses a risk to aid delivery. For example, if a medical record for a child is incorrect due to data entry errors, that child may receive the wrong vaccination or be denied necessary food rations.
- **Third-Party Transfer Risks:** UNICEF frequently partners with local NGOs and commercial vendors to implement programs. There is an inherent risk that these third parties may not adhere to the same high standards of privacy as UNICEF. Without strict contractual clauses and monitoring, data shared with partners effectively leaves our control.

7. Responsibilities

7.1 Governance Structure To effectively manage the risks outlined above, UNICEF has established a clear chain of command and responsibility regarding data privacy. Privacy is not solely the domain of the IT department; it is a shared responsibility across the entire organization.

7.2 Key Roles and Officers The following roles have specific, mandated responsibilities under this policy:

- **Privacy Leader (Executive Director / Deputy Executive Directors):** The senior leadership team is responsible for setting the "tone at the top." They must approve the privacy strategy, allocate sufficient budget for privacy initiatives, and ensure that data protection is integrated into the organization's overall risk management framework.
- **Data Protection Officer (DPO):** The DPO is the primary authority on privacy within UNICEF. Their responsibilities include:
    - Monitoring internal compliance with this policy and international laws (such as GDPR).
    - Acting as the point of contact for data subjects (donors/staff) who wish to exercise their rights.
    - Conducting Data Protection Impact Assessments (DPIAs) for new projects.
    - Reporting serious breaches to the senior leadership and relevant authorities.
- **IT Managers and Security Officers:** Information Technology managers are responsible for the technical implementation of privacy controls. This includes:
    - Ensuring encryption of data at rest and in transit.

    - Managing access controls (passwords, multi-factor authentication) to ensure only authorized staff can view PII.
    - Maintaining firewalls and intrusion detection systems to prevent external hacks.
- **Marketing and Fundraising Managers:** Staff involved in donor relations have specific responsibilities regarding donor data:
    - Ensuring that marketing emails are only sent to those who have opted in.
    - Managing the "unsubscribe" lists to ensure we do not contact donors who have asked to be removed.
    - Protecting the financial details of donors during fundraising campaigns.
- **Country Representatives (Field Offices):** The Head of Office in each country is responsible for ensuring that their local staff adhere to this policy. They must also contextualize these rules to fit local laws and customs, ensuring that data collection does not violate local cultural norms.

7.3 General Staff Guidelines All UNICEF employees, regardless of their specific role, are considered "data stewards." Every staff member has the following baseline responsibilities:

- **Confidentiality:** Staff must never share PII (login credentials, donor lists, beneficiary files) with unauthorized persons, including family members or friends.
- **Vigilance:** Staff must report any suspected data breach or security incident to the DPO immediately.
- **Clean Desk Policy:** Physical documents containing PII must not be left unattended on desks and must be locked away when not in use.
- **Phishing Awareness:** Staff must remain vigilant against email phishing attacks that attempt to steal credentials to access UNICEF databases.

8. Requirements for PII: Storage

8.1 Digital Storage Standards UNICEF mandates strict technical protocols for the storage of PII to ensure its confidentiality and integrity while "at rest" (stored on servers or devices).

- **Encryption Standards:** All databases containing Sensitive PII (SPII), including donor financial data and beneficiary medical records, must be encrypted using the Advanced Encryption Standard (AES) with 256-bit keys. This ensures that even if physical servers are stolen, the data remains unreadable without the decryption key.
- **Server Locations:** Primary data centers must be located in jurisdictions with adequate data protection laws. For field operations, local servers must be kept in secure, climate-controlled environments with backup power supplies.
- **Access Control Mechanisms:** Access to stored PII is governed by the Principle of Least Privilege (PoLP). Access rights are granted based on the user's role, not their seniority.
    - **Role-Based Access Control (RBAC):** Users are assigned specific roles (e.g., "Field Medic," "Donor Relations Officer") which grant access only to the data partitions necessary for that job.
    - **Multi-Factor Authentication (MFA):** Access to any cloud-based storage system or internal database containing PII requires MFA (e.g., a password plus a code sent to a mobile device).

8.2 Physical Storage Standards While UNICEF is digitally transforming, paper records remain common in field operations.

- **Secure Filing:** Physical files containing PII (such as paper intake forms for refugees) must be stored in lockable metal filing cabinets. Keys must be held only by authorized personnel.
- **Clean Desk Policy:** No file containing PII shall be left on a desk overnight. At the end of the workday, all documents must be returned to secure storage.
- **Device Security:** All UNICEF-issued laptops and mobile tablets used in the field must be physically secured when not in use. They must be equipped with remote-wipe software to destroy data if the device is lost or stolen.

9. Requirements for PII: Data Use

9.1 Protection During Transmission (Data in Transit) Data is most vulnerable when it is moving between locations.

- **Secure Protocols:** All transmission of PII over public networks (the internet) must be secured using Transport Layer Security (TLS 1.2 or higher). Unencrypted transmission (HTTP) of PII is strictly prohibited.
- **Email Security:** Highly sensitive PII (such as HIV status or passport scans) should not be sent via standard email bodies. Instead, such data should be placed in a password-protected attachment, with the password communicated via a separate channel (e.g., a phone call or secure chat).
- **VPN Requirement:** Staff accessing UNICEF networks remotely (from hotels, airports, or home) must use the official UNICEF Virtual Private Network (VPN) to create an encrypted tunnel for their traffic.

9.2 Anonymization for Research UNICEF frequently uses data for research and advocacy reports.

- **De-identification:** Before PII is used for statistical analysis or external reporting, it must be de-identified. Names, exact addresses, and other direct identifiers must be stripped from the dataset.
- **Aggregation:** Whenever possible, data should be aggregated (e.g., "50 children in the region" rather than individual names) to prevent re-identification of specific subjects.

10. Data Accuracy

10.1 Maintenance of Integrity UNICEF acknowledges that outdated or incorrect data can harm beneficiaries and irritate donors.

- **Employee Responsibilities:** It is the duty of every employee entering data to verify its accuracy at the point of collection. For example, field staff must repeat names and dates of birth back to beneficiaries to confirm spelling.
- **Regular Audits:** Data owners (department heads) are required to conduct annual audits of their datasets. Records that are incomplete or clearly erroneous must be flagged for correction or deletion.

10.2 Rectification Protocol

- **Donor Updates:** The fundraising division must provide an easy mechanism for donors to update their contact information and preferences.

- **Beneficiary Records:** In long-term aid programs, beneficiary status must be reviewed every 6 months to ensure that the aid is still required and that the family composition (births/deaths) is accurately reflected in the database.

11. Data Breach Incident Response Protocol

11.1 Purpose Despite robust preventive measures, the risk of a data breach cannot be entirely eliminated. This section outlines the mandatory steps UNICEF staff must take in the event of a suspected or confirmed privacy incident. This protocol is designed to minimize impact, preserve evidence, and ensure compliance with notification obligations.

11.2 Phase I: Identification and Reporting

- **Immediate Trigger:** Any staff member who suspects a breach (e.g., lost laptop, accidental email to wrong recipient, suspicious server activity) must report it immediately.
- **Reporting Channel:** Reports must be made via the internal "Red Button" on the UNICEF intranet or via the 24/7 Security Hotline (+1-212-555-0199).
- **No Retaliation:** UNICEF maintains a non-punitive reporting culture. Staff who report errors in good faith will not face disciplinary action for the report itself.

11.3 Phase II: Containment and Eradication

- **Isolation:** The IT Security Team (CSIRT) will immediately isolate the affected systems to prevent the spread of the attack. This may involve disconnecting servers from the internet or disabling compromised user accounts.

- **Preservation of Evidence:** Logs and audit trails must be preserved for forensic analysis. Staff are instructed not to turn off or reboot infected machines unless directed by IT Security.

11.4 Phase III: Risk Assessment

- **Severity Scoring:** The Data Protection Officer (DPO) will convene the Privacy Board to assess the severity of the breach based on:
    1. **Nature of Data:** Was it basic PII or Sensitive PII (medical/financial)?
    2. **Volume:** How many individuals are affected?
    3. **Context:** Does this put beneficiaries in physical danger?
- **Determining Notification:** Based on the score, the DPO will determine if notification to regulators and data subjects is required.

11.5 Phase IV: Notification

- **Regulatory Notification:** If the breach poses a risk to the rights and freedoms of individuals, UNICEF will notify the relevant data protection authorities (such as the EDPS for EU operations) without undue delay and, where feasible, not later than 72 hours after having become aware of the breach.
- **Data Subject Notification:** If the breach is likely to result in a high risk to the rights and freedoms of natural persons, UNICEF shall communicate the personal data breach to the data subject without undue delay. This communication will be in clear and plain language.

11.6 Phase V: Post-Incident Review

- **Lessons Learned:** Within 30 days of closing an incident, the CISO must submit a "Lessons Learned" report to the Executive Director.
- **Policy Update:** If the breach was caused by a gap in policy, this document must be updated immediately to close that gap.

12. Executive Sign-Off

Approval of Policy By signing below, the senior leadership of UNICEF acknowledges the critical importance of this Information Privacy Policy. We commit to providing the necessary resources, authority, and support to the Data Protection Officer and all staff to ensure full implementation of these standards. We affirm that the protection of privacy is integral to the protection of children's rights.

This policy is effective immediately upon signature.

Catherine Russell Executive Director UNICEF

Date: 12/7/25

Thomas Davin Director, Office of Global Insight and Policy UNICEF

Date: 12/7/25

Kaan Cetinturk Chief Information Officer (CIO) UNICEF IT Division

Date: 12/7/25
