DATA PROTECTION POLICY

Approved on:	2024-May-01
Approved by:	Executive Board
Version:	2.1
Prepared by:	Legal & Compliance
Review Cycle:	2 Years
Next revision:	2025
Contact Person:	Legal & Compliance Compliance@welthungerhilfe.de
Binding on:	■ All employees of Welthungerhilfe (Deutsche Welthungerhilfe e.V. ("**Association**") und Deutsche Welthungerhilfe Foundation ("**Foundation**"; Association and Foundation collectively, "**Welthungerhilfe**" or "**WHH**")

The current applicable version of this document is available on the webpage www.welthungerhilfe.org/code-of-conduct.

Table of contents

1. Introduction

Welthungehilfe processes *Personal Data* in a variety of ways in order to successfully carry out its organisational purposes. Personal Data is highly personal. It allows direct conclusions to be drawn about the individuals behind it (the "***Data Subjects***"). Therefore, the improper *Processing of Personal Data* can cause serious violations of the private rights of *Data Subjects* and can lead to grave harm both for them and for *Welthungerhilfe*. Accordingly, Welthungerhilfe takes the protection of *Personal Data* very seriously. Effective protection requires a clear allocation of data protection-related responsibilities within *Welthungerhilfe*. This Data Protection Policy ("***Policy***") allocates responsibility for data protection and establishes clear rules of conduct for *WHH Employees*.

2. Objectives

The objectives of this *Policy* are as follows:

- to safeguard the fundamental rights and freedoms of *Data Subjects*, in particular, their right to the protection of *Personal Data*, and to ensure an adequate level of protection of the *Processing of Personal Data* by *Welthungerhilfe* through general organisational measures and the allocation of responsibilities;
- to create minimum standards and a uniform framework for the use and protection of *Personal Data* within *Welthungerhilfe*;
- to implement the "do-no-harm-principle" in line with the Core Humanitarian Standard on Quality and Accountability throughout our humanitarian aid and development cooperation activities consistently also with respect to the protection of Personal Data;
- to strengthen *Welthungerhilfe's* position as a professional and trustworthy organisation, to strengthen confidence in its activities, and to prevent damage to *Welthungerhilfe*'s image and brand; and
- to ensure compliance with existing legal, contractual, and other obligations[1] through guidelines for *WHH Employees* and through the clear allocation of responsibilities.

This *Policy* shall at all times be easily accessible to all *WHH Employees*.

3. Scope

The standards of this *Policy* apply to the following:

a) the executive board of the Association, the Foundation's management, and all other employees of *Welthungerhilfe*, regardless of their type of contract (including, among others, full-time employees, temporary personnel, trainees, and personnel on loan), the scope of their responsibilities, and the location of their employment (collectively, "**WHH Employees**"); and
b) Social businesses in which *Welthungerhilfe* has a share of more than 50%.

The requirements and prohibitions of this *Policy* apply to all handling of *Personal Data*, regardless of whether it is electronic, in hard copy (paper form), or in any other form.

[1] E.g., laws and statutes (such as the EU General Data Protection Regulation (or "**GDPR**") and the German Federal Data Protection Act), grant awards by institutional donors (including ancillary provisions), and other international standards binding on Welthungerhilfe (e.g., the Core Humanitarian Standard).

Furthermore, it covers all types of *Data Subjects* (including, among others, donors, WHH Employees, suppliers, employees of partner organisations, *Project Participants*).

This *Policy* applies worldwide as a minimum standard for all *WHH Employees*. It is to be understood in connection with *Welthungerhilfe*'s Code of Conduct and the policies and international standards and codes mentioned therein. In addition, *WHH Employees* must comply with the laws and regulations applicable in their work location. The stricter standards always apply. Should any local law or regulation contradict this Policy, the responsible *Country Management* will inform the *Global Privacy Officer* in writing and agree on a solution that is in line with this Policy. Deviations from this *Policy* are only permitted with the prior written consent of the responsible *Country Management* in consultation with the *Global Privacy Officer*.

The Association's Executive Board and the Foundation's management are each responsible for implementation of this *Policy* within Germany and at the global level, as well, in general, for compliance with data protection standards within their organisations.

Each *Country Management* is separately responsible for implementing this *Policy* in its respective programme country. It must stay informed about current country-specific data protection requirements and take these into account, as appropriate.

4. Definitions

Definitions have the same core meaning throughout this policy, regardless of the word form in which they are used[2]; they are set in italics for ease of identification.

4.1. Anonymisation

Anonymisation is the *Processing of Personal Data* in a way that ensures that the data does not refer to an identified or identifiable natural person or that the *Data Subject* is not identifiable – even indirectly by consulting other information.

4.2. Application Owner

For software applications that require special data protection support, an *Application Owner* shall be named in the place where the software is operationally managed. In accordance with clause 6.3.4, the *Application Owner* ensures that concerns related to data protection are adequately accounted for during development and operation of the software application and serves as an internal contact person for data protection issues related to the software application

4.3. Association

Deutsche Welthungerhilfe e.V., VR 3810, Friedrich-Ebert-Str. 1, 53173 Bonn.

4.4. Biometric Data

Biometric Data is *Personal Data* resulting from specific technological processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data.

[2] For example, the terms "processing," "processed," and "data processing" have the same defined core meaning.

4.5. Consent

Consent of the *Data Subject* is any freely given expression of will through which the *Data Subject* indicates their agreement to the *Processing* of *Personal Data* related to them in a specific case. Such *Consent* must be provided in an informed and unambiguous manner, in the form of a declaration or another unambiguous confirming act.

4.6. Controller

The *Controller*[3] is the natural or legal person, public authority, institution, or other body that, alone or jointly with others, determines the purposes for and means of *Processing* of *Personal Data*. The *Association*'s *Controller* is Deutsche Welthungerhilfe e.V.; the *Foundation*'s *Controller* is Deutsche Welthungerhilfe Foundation.

4.7. Country Management

The *Country Management* is the executive management function for a particular country. In Germany, this is the executive board / management of WHH. In programme countries, this is the respective country director. If more than one country director is appointed in a country, they are collectively considered the *Country Management*. If *Projects* are carried out in a country that does not have an established *Country Office*, it must be determined during the planning of these *Projects* who will perform the tasks and duties of the *Country Management* under this *Policy* in relation to these *Projects*.

4.8. Country Office

The office established and usually accredited abroad) in a programme country that, among other things, coordinates and/or is responsible for the preparation and implementation of programmes and *Projects* assigned to that country.

4.9. Country Privacy Officer

Each *Country Management* should appoint a *Country Privacy Officer* for its *Country Office*. The *Country Privacy Officer* is responsible for performing the tasks described in clause 5.3.1 in the respective *Country Office*. If the *Country Management* does not appoint a *Country Privacy Officer*, the *Country Management* remains responsible for these duties.

4.10. Data Breach

Data Breach means a breach of security of *Personal Data* that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *Personal Data* processed by or on behalf of *Welthungerhilfe*.

4.11. Data Incident Response Team

A *Data Incident Response Team* shall be established in the *Head Office* and will include, at a minimum, the following functions: the *Global Privacy Officer*, the head of IT, and the information security and data protection expert. The *Global Privacy Officer* may invite other individuals to take part in the *Data Incident Response Team* as needed under the circumstances of the specific case. If a serious *Data Breach* occurs in a *Country Office*, the *Data Incident Response Team* must consult the Country Privacy Officer in that *Country Office*. In the event of a suspected or confirmed serious *Data Breach*, the *Data Incident Response Team* is tasked with determining appropriate measures to minimize the damages caused by the *Data Breach*, to immediately intercept and remedy the *Data Breach*, to inform relevant affected persons and/or supervisory authorities, and to prevent future *Data Breaches*.

[3] "Controller" under GDPR art. 4(7).

4.12. Data Processor
A *Data Processor* is a natural or legal person, public authority, agency, or other body that processes *Personal Data* on behalf of the *Controller*.

4.13. Data Protection Officer
The *Data Protection Officer* is a function established by the *Head Office* or a *Country Officer* under applicable mandatory law that assists in ensuring compliance with data protection requirements.

4.14. Data Subject
Any natural person who is identified in or identifiable on the basis of *Personal Data*, such as a donor, *WHH Employee*, supplier, employee of a partner organisation, or *Project Participant*.

4.15. Department
A permanent and autonomous functional unit or department of the *Head Office* or a *Country Office* that is depicted on the corresponding organigram of the *Head Office/Country Office* (e.g., Finance, Human Resources, Logistics, Internal Audit, Communication).

4.16. Foundation
Stiftung Deutsche Welthungerhilfe, Friedrich-Ebert-Str. 1, 53173 Bonn.

4.17. General Data Protection Regulation ("GDPR")
Regulation (EU) 2016/679 (General Data Protection Regulation), as currently amended (OJ L 119, 04.05.2016; OJ L 127, 23.05.2018).

4.18. Genetic Data
Genetic Data is *Personal Data* related to the inherent or acquired genetic characteristics of a natural person that provides unique information about the physiology or the health of that natural person and is obtained, in particular, from an analysis of a biological sample of the natural person in question.

4.19. Global Privacy Officer
The Association's executive board appoints a *Global Privacy Officer* for *Welthungerhilfe* in consultation with the Foundation's management. The *Global Privacy Officer* reports directly to the executive board; for matters that concern the Foundation only, they report directly to the Foundation's management. They perform their tasks described in clause 5.3.2 independently and based on their expertise.

4.20. Head Office
Welthungerhilfe's operations in Bonn and Berlin.

4.21. International Organisation
An *International Organisation* is an organisation established under international law, along with its subordinate bodies, or any other body that is set up by, or based on, an agreement between two or more countries.

4.22. Personal Data
Personal Data means any information relating to a Data Subject, such as donor data, data of implementing partners and Project Participants, and personnel data of WHH Employees. It is

sufficient if the information in question is linked to the name of the Data Subject or a connection can be established independently based on the context, even if the information must first be linked to additional knowledge.[4]

4.23. Policy
This Data Protection Policy in its respective current version.

4.24. Processing
Processing is any operation or set of operations, whether or not automated, performed upon *Personal Data*, such as collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing through transmission, disseminating or otherwise making available, aligning or combining, *Restricting*, erasing, or destroying. For example, not only does the collection of *Personal Data* from *Project Participants* constitute *Processing*, but also the mere display of *Personal Data* on an electronic tablet constitutes disclosure and is therefore *Processing*.

4.25. Processing Restriction
A *Processing Restriction* is the marking of stored *Personal Data* with the aim of limiting its future *Processing*.

4.26. Profiling
Profiling means any form of automated *Processing* of *Personal Data* consisting of the use of *Personal Data* to evaluate certain personal aspects related to a natural person, in particular, to analyse or predict that person's performance at work, economic situation, health, physical state, nutritional status, personal preferences, interests, reliability, behaviour, location, or movement.

4.27. Project
A temporary organisational unit equipped with an own budget and set up for the purpose of implementing specific humanitarian aid or development cooperation activities in a programme country and normally led by a head of project.

4.28. Project Participants
Project Participants are target groups of programmes and *Projects* implemented by *Welthungerhilfe* or its partner organisations; members of communities in which *Welthungerhilfe* and its partner organisations are active; and all other individuals who are actively participating in the programmes or *Projects* of *Welthungerhilfe* or its partner organisations, and are not *WHH Employees* or employees of a partner organisation.

4.29. Pseudonymisation
Pseudonymisation is the *Processing* of *Personal Data* in such a manner that the *Personal Data* can no longer be attributed to specific *Data Subjects* without additional information, provided that this additional information is stored separately and is subject to technical and organisational measures that ensure the *Personal Data* is not attributable to an identified or identifiable natural person.

[4] For example, the name of a contact person can be used to identify a natural person, as can the person's e-mail address or the IP address of a website visitor. Photos, videos, and audio recordings also constitute Personal Data.

4.30. Recipient
The *Recipient*[5] is any natural or legal person, public authority, institution, or other body to which *Personal Data* is disclosed, regardless of whether that person is a *Third Party*.

4.31. Sensitive Personal Data
Sensitive Personal Data[6] is information that may reveal a natural person's ethnic or other origin,[7] political opinions, religious or philosophical beliefs, or trade union membership, as well as Genetic Data or Biometric Data for the purpose of uniquely identifying a natural person, data concerning health, or concerning a natural person's sex life or sexual orientation.

4.32. Third Party
Third Parties are natural or legal persons, public authorities, institutions, or other bodies other than the *Data Subject*, the *Controller*, the *Data Processer*, and other persons who have direct authorisation from the *Controller* or the *Data Processor* to process *Personal Data*.

4.33. Welthungerhilfe or WHH
Deutsche Welthungerhilfe e.V. and the Welthungerhilfe Foundation, insofar as this *Policy* applies to both cumulatively or alternatively.

4.34. WHH Employee
The Association's board of directors, the Foundation's board and management, and all other employees of Welthungerhilfe, regardless of the type of contract (including, among others, full-time employees, temporary personnel, trainees, and personnel on loan) and the scope and location of their employment.

5. Data Protection: Organisational Structure

5.1. General Organisation
The overall responsibility for data protection lies globally with the WHH executive board and for each country with the *Country Management*. The *Global Privacy Officer* and the *Country Privacy Officers*, respectively, support the executive board and the Country Management in performing their respective duties.

5.2. Overall Responsibility in Programme Countries
Each *Country Management* is responsible for complying with data protection laws and regulations pertaining to the respective *Country Office*. In addition, it must ensure that managers, *WHH Employees*, and *Third Parties* (including partner organisations) that *process Personal Data* under the responsibility of the *Country Office* are informed in accordance with *GDPR* and local requirements and, where necessary, receive appropriate training.

5.3. Definition of Responsibilities
Within its area of responsibility, the *Country Management* shall clearly define the roles and responsibilities relating to the handling of *Personal Data* and shall regularly monitor and

[5] "Recipient" under GDPR art. 4(9).
[6] Art. 9 GDPR uses the term "special categories of personal data." The term "Sensitive Personal Data" used in the Policy for reasons of clarity has the same meaning.
[7] The *Policy* intentionally does not use the term "racial origin" as used in the GDPR in order to clarify that *Welthungerhilfe* rejects any theories that attempt to prove the existence of different human races. A restriction of the legal definition is not intended.

document the execution of those. The Country Management may appoint a *Country Privacy Officer* to provide support. If a *Country Privacy Officer* is not appointed, the *Country Management* shall remain responsible for the duties of the Country Privacy Officer.

When defining roles and responsibilities relating to the handling of Personal Data, the following criteria shall be taken into account:

5.3.1. Country Privacy Officer

The *Country Privacy Officer* is responsible for supporting compliance with data protection requirements within the area of responsibility of the respective *Country Office*. In addition, they are responsible for aligning data protection issues with this *Policy* in the respective country. They also serve as the contact person for the *Head Office* and the *Global Privacy Officer* and provide them with information on data protection-related issues of the *Country Office*. Where required by law, a *Data Protection Officer* must also be appointed for the *Country Office*; this person may also perform the duties of the *Country Privacy Officer*. The *Global Privacy Officer* is the technical manager of the *Country Privacy Officers*; the disciplinary manager is the *Country Management*. Disciplinary measures against *Country Privacy Officers* require the prior consent of the *Global Privacy Officer*.

5.3.2. Global Privacy Officer

The *Global Privacy Officer* receives reports from the *Data Protection Officer* on behalf of the WHH executive board or the management of the Foundation and forwards them accordingly. In addition, he Global Privacy Officer supports the Association's executive board, the Foundation's management, the *Country Offices*, and the *Country Privacy Officers* in their respective duties, including, among other things, by specifying procedures and templates. Furthermore, the *Global Privacy Officer* coordinates data protection issues that have relevance to WHH as a whole. The *Global Privacy Officer* is the technical manager of the *Country Privacy Officers*.

5.3.3. Data Protection Officer

Welthungerhilfe has appointed a statutory *Data Protection Officer* at the *Head Office*. The *Data Protection Officer* can be reached through the following means:

- Email: data.protection@welthungerhilfe.de,
- By mail: Deutsche Welthungerhilfe e.V., "Attn: Data Protection Officer," Friedrich-Ebert-Str. 1, 53173 Bonn-Bad Godesberg, Germany

The *Data Protection Officer* monitors compliance with the *GDPR* and other statutory or regulatory requirements, including the requirements of this and other *Welthungerhilfe* data protection policies. The *Data Protection Officer* advises and informs the executive board and the Foundation's management regarding existing data protection obligations and is responsible for communicating with supervisory authorities. The Data Protection Officer checks selected processes at appropriate intervals on a random, risk-oriented basis to ensure their conformity with data protection guidelines.

The *Data Protection Officer* performs their duties independently and based on their special expertise. They report directly to the *Global Privacy Officer*. In the event of an emergency, unavailability of the *Global Privacy Officer*, or the need to report directly to the executive board or the management of the Foundation, the *Data Protection Officer* may also report directly to the executive board or the management of the Foundation. In such an instance, a copy must be provided to the *Global Privacy Officer*, unless there are compelling reasons not to do so.

All Departments and all *WHH Employees* shall support the Data Protection Officer in the performance of their duties.

6. General Principles and Procedures

6.1. Information Security Framework: Availability, Confidentiality, and Integrity of Data

6.1.1. General Information Security Framework

To ensure the availability, confidentiality, and integrity of information, a general security framework shall be prepared based on the Information Security Policy and in reliance on a risk analysis identifying protection needs, and shall set forth binding procedures for *Processing* information, including the *Processing* of *Personal Data*. The state of the art must be particularly considered in this framework.

The security framework shall be regularly reviewed and evaluated with regard to the effectiveness of the technical and organisational measures provided for therein. A classification system shall be established for the handling of information. All *WHH Employees* shall be appropriately sensitised, including through trainings, with regard to the careful handling of information, in particular, confidential and sensitive information, including *Personal Data*. The Information Security Policy regulates these issues in detail.

6.1.2. Risk Assessment on the Processing of Personal Data

Taking into account the type, scope, circumstances, and purposes of *Processing* and the probability of a *Data Breach*, each *Department* responsible for *Processing Personal Data* shall determine the need for protection of *Processing* itself and the data processed therein with a view towards the consequences of a potential *Data Breach* for the *Data Subjects* (see also parts 6.3.2 (General Risk Assessment) and 6.3.3 (Data Protection Impact Assessment)). In this regard, the *Country Privacy Officer*, the *Global Privacy Officer*, or the *Data Protection Officer* can be consulted.

6.1.3. Obligation of Data Confidentiality

WHH Employees are prohibited from *Processing Personal Data* without authorisation. They must commit to treat Personal Data confidentially before taking up their employment duties. This obligation is made using a form provided for this purpose. *WHH Employees* with special secrecy obligations must also agree to any such additional obligation in writing.

6.1.4. Special Security Measures for the Processing of Personal Data

The requirements of the Information Security Policy must be followed. Access to *Personal Data* should only be granted to those persons who need to access the data in order to perform their duties ("**Need-to-know Principle**"). Authorisations to access data must be precisely and completely stipulated and documented, regularly checked, and, if necessary, updated. Transfers of *Personal Data* through public networks shall be encrypted whenever possible. Encryption is mandatory if required by the need for protection.

Personal Data collected for different purposes shall be *processed* separately. The separation of data shall be ensured by appropriate technical and organisational measures.

It must be ensured that service providers cannot access *Personal Data* without authorisation. Remote maintenance access is only to be granted in individual cases and must follow the principle of minimal rights assignment. Remote maintenance activities shall be recorded or logged, if possible.

6.2. Register of Processing Activities

6.2.1. Obligation to Maintain a Register

The *Head Office* and each *Country Office* of *Welthungerhilfe* shall maintain a register of all *Processing* activities of *Personal Data*. Each *Department /Project* shall name an individual who will document and maintain all necessary information on the procedures of the respective unit, in accordance with the legal requirements and this *Policy*. The *Data Protection Officer* or the (*Global/Country*) *Privacy Officers* may be consulted for advice.

6.2.2. Consolidated Register

The registers of the *Country Offices* and the *Head Office* shall be consolidated in an appropriate manner in a complete register and checked at regular intervals for accuracy, completeness, and consistency.

6.2.3. Submission

Welthungerhilfe will make the register available to the supervisory authority upon request. The *Data Protection Officer* is responsible for this, in coordination with the *Global Privacy Officer*.

6.3. General Organisational Measures

6.3.1. Responsibility in Handling Personal Data

The tasks und responsibilities for handling *Personal Data* shall be clearly defined and their implementation shall be regularly monitored and documented.

6.3.2. General Risk Assessment

Each *Country Office* shall regularly assess data protection risk, including associated reputational risk, and evaluated them in terms of their possible repercussions on business processes. The results of this risk assessment must be documented and – if material to *Welthungerhilfe* – incorporated into central risk management.

6.3.3. Data Protection Impact Assessment

If a *Department* or *Project* processes *Personal Data* under its own responsibility and such *Processing* may pose a high risk to the rights or freedoms of *Data Subjects*, the *Department* or *Project* must carry out a data protection impact assessment before the *Processing* begins. This particularly applies to the *Processing* of *Personal Data* of vulnerable *Project Participants*. Such a high risk exists, for example, if a large amount of *Personal Data* is being processed by default, if extensive *Processing* of *Sensitive Personal Data* is to be carried out, if a comprehensive and systematic evaluation of personal characteristics of *Data Subjects* is to occur, or if the *Processing* operations are likely to present a very high risk to a *Data Subject* in any other way. A data protection impact assessment is also required if new data processing technologies are to be introduced. The data protection impact assessment must be documented in writing and include, at a minimum, the following content:

- a systematic description of the envisaged *Processing* activity and the purpose of such *Processing*, including, where appropriate, the legitimate interests pursued by the *Controller*;
- an assessment of the necessity and proportionality of the *Processing* activity in relation to the purpose; and

- an assessment of the risks to the rights and freedoms of *Data Subjects* and the safeguards to be taken to address those risks, including safety precautions, security measures, and procedures designed to ensure the protection of *Personal Data*.

The *Data Protection Officer* shall advise the *Department/Project* carrying out the data protection impact assessment and on when *Processing* activities may present a high risk to *Data Subjects*.

6.3.4. *Application Owner* for Privacy Intensive Software Applications

For software applications that require special data protection attention, an *Application Owner* shall be named who works where the software application is operationally managed. The *Application Owner* shall ensure that concerns related to data protection are adequately accounted for during development (see part 6.3.5) and operation of the software application. They also serve as an internal contact person for data protection issues related to the software application. Such software applications are, as a rule, (i) websites and apps, (ii) IT systems through which large amounts of *Personal Data* are processed (donor and user administration, business information, donor relationship management, whistleblower systems), (iii) the administration of *Consents* (opt-ins) and objections (opt-outs), and (iv) the *Processing* of data from *WHH Employees* or *Project Participants*, health data, bank/credit card data, and other *Sensitive Personal Data*.

6.3.5. Development, Procurement, and Use of Business Models and IT Systems for *Processing Personal Data*

When developing business models and IT systems that process personal data, the legal and technical requirements of data protection (including "**Privacy by Design**" and "**Privacy by Default**") must be taken into account, starting at the design stage. In particular, this includes appropriate and current technical requirements, technical and organisational measures, default settings friendly to Data Protection, the separation and encryption of data, and the creation of and compliance with a procedure for storing, maintaining, and deleting data. The principle of data minimisation (see part 7.2) shall be observed.

When selecting and designing data *Processing* systems, data protection must be integrated into the specifications and architecture of data *Processing* systems from the outset in order to facilitate compliance with the principles of privacy and data protection, including the principle of data minimisation. The use and default settings of data *Processing* systems shall be designed to take the principle of data minimisation into account.

7. General Handling of *Personal Data*

7.1. *Processing* Only on the Basis of with Legal Authorisation

The *Processing* of *Personal Data* is generally prohibited, unless explicitly permitted by law. In general, the *GDPR* allows for the *Processing* of *Personal Data* if and to the extent that one of the following applies:

- It is necessary for the performance of an existing contractual relationship with the *Data Subject*.
  Example: The storage of necessary *Personal Data* within the framework of a consultancy contract or an employment relationship.
- It is necessary in the course of pre-contractual measures at the *Data Subject*'s request and in the course executing a contract with the *Data Subject*.
  Example: Interested donor requests informational materials or verification of the general

use of donations and then decides to donate. The data required to send the information and to process the donation (e.g., data for issuing and sending the donation receipt) may be processed.

- The *Data Subject* has given their voluntary and informed *Consent*.
  Example: The *Data Subject* voluntarily registers to receive a newsletter or a *Project Paticipant* agrees to the *Processing* of their data by use of a cash card system.
- *Welthungerhilfe* is subject to a legal obligation.
  Example: Legal data retention periods under the German Commercial Code or the German Fiscal Code.
- The *Processing* is necessary to protect a vital interest of the *Data Subject* or of another individual.
  Example: *Processing* for huminatrian purposes, including the monitoring of epidemics and their spread, or in situations of humanitarian emergencies, in particular, natural or man-made disasters.
- Where *Welthungerhilfe* has a legitimate interest in *processing* the data that is not overridden by the interests or fundamental rights of the *Data Subject*, especially in the case of a child. However, data *Processing* based on a legitimate interest should not be carried out without prior documented advice from the *Data Protection Officer* or the *Country* or *Global Privacy Officer*.
  Example: The use of the postal address of active donors to send out promotional letters.

7.2. Principle of Data Minimisation

The *Processing* of *Personal Data* shall be aimed at *Processing* as little data as possible from *Data Subjects*. *Personal Data* may only be *processed* to the extent necessary to achieve the legitimate purpose of the *Processing*. In particular, *Personal Data* must be *anonymised* or *pseudonymised* as far as this is possible, based on the purpose of use. For example, it will usually not be necessary to know and use the names of *Data Subjects* in the context of a statistical evaluation of data. Rather, this information can be replaced by a random value that also ensures that the underlying information is distinguishable.

7.3. Specifying a Clear *Processing* Purpose

Personal Data may only be *Processed* for a specified, explicit, and legitimate purpose. Data *Processing* without a legitimate purpose, such as the storage of data by default, is not allowed.

7.4. Changing the *Processing* Purpose

Processing of Personal Data for a purpose other than that for which the Data Subject provided previous Consent is only allowed if the purpose of the further *Processing* is compatible with the purpose covered by the original *Consent*. In particular, the reasonable expectations of the *Data Subject* vis-à-vis *Welthungerhilfe* with regard to such further *Processing*, the nature of the data processed, the consequences for the *Data Subject*, and the possibilities of encryption or *Pseudonymisation* must be taken into account. The *Data Subject* must be fully informed about any change in the *Processing* purpose. The *Data Protection Officer* shall advise on the appropriate scope of the duty to inform.

7.5. Adequately Informing *Data Subjects*

When *Personal Data* is collected, *Data Subjects* shall be adequately informed about how their data will be handled. The information must include the purpose of the *Processing*, the identity of the *Controller*, the *Recipients* of the *Personal Data*, and all other information necessary to

ensure fair and transparent *Processing*. The information shall be prepared in an understandable and easily accessible form and in as simple language as possible. In cases of doubt, the *(Global/Country) Privacy Officer* shall agree with the *Data Protection Officer* on the appropriate scope of information that must be provided and shall document the result of this agreement.

7.6. Data Collection from *Third Parties* /Subsequent Change of the *Processing* Purpose

If *Personal Data* is not collected from the *Data Subject*, but is procured, for example, from another company, the *Data Subject* must be subsequently and comprehensively informed about how their data is handled. The *Data Protection Officer* shall advise on the appropriate scope of the duty to inform.

7.7. Data Integrity

As far as possible with reasonable effort, *Welthungerhilfe* shall ensure that *processed Personal Data* is factually correct and, if necessary, up to date. The extent of data *Processing* must be necessary and relevant in relation to the specified *Processing* purpose. The responsible *Department/Project* shall ensure data integrity by establishing appropriate processes and regularly reviewing databases in an appropriate manner to ensure that they are correct, necessary, and up to date.

8. Sensitive Personal Data

8.1. Special Processing Requirements

In principle, *SensitivePersonal Data* (see part 4.14) may only be processed with the *Consent* of the *Data Subject* or, in rare cases, based on specific, explicit legal authorisation. Furthermore, additional technical and organisational measures (e.g., encryption during transport, minimal assignment of rights) must be taken to protect *SensitivePersonal Data* in every *Processing* operation. The revocation of *Consent* by the *Data Subject* is possible and must be observed.

8.2. Duty to Disclose

If a *Department*, *Project*, or *Country Office* intends to *Process SensitivePersonal Data*, the responsible *Department*, *Project*, or *Country Office* must notify the *Global Privacy Officer* and the *Data Protection Officer* in writing and in good time in advance of the intended *Processing* (if possible as early as the time of the project application). The necessity of the *Processing* must be justified; likewise, the special technical and organisational measures to be applied during the *Processing* to protect the *Sensitive Personal Data* must be presented transparently.

9. Data Transfers

9.1. Special Permission

The transmission of *Personal Data* to *Third Parties* is only allowed based on law or on the *Consent* of the *Data Subject*.

9.2. Transfer to Countries outside of the European Union/EEA or to *International Organisations*

If the *Recipient* of *Personal Data* is located outside the European Union or the European Economic Area, or if the *Recipient* is an *International Organisation*, additional measures are required to safeguard the rights and interests of *Data Subjects*. A data transfer should not occur if an adequate level of data protection is not available at the receiving body or cannot be established – for example, by means of a special contractual clause.

10. External Service Providers as *Data Processors*

10.1. Access to *Personal Data* by External Service Providers

If external service providers are to have access to *Sensitive Personal Data*, the *Data Protection Officer* must be informed in advance. In this regard, the special requirements of part 6.1.4 of this *Policy* (relating to remote maintenance) must also be observed.

10.2. Due Diligence Obligation

Service providers with possible access to *Personal Data* must be carefully vetted before they are engaged. The selection process must be documented and should, in particular, take the following factors into account:

- professional suitability of the service provider for the specific data handling;
- technical and organisational security measures assured by the service provider;
- experience of the service provider in the market; and
- other factors that indicate the reliability of the service provider (e.g., data protection documentation, level of safeguards, willingness to cooperate, response times).

10.3. Order Processing

Should service providers be engaged to *process personal data* on behalf of *Welthungerhilfe*, a contract for *processing* activities must be concluded. The contract shall appropriately regulate data protection and IT security, taking into account GDPR articles 27, 28, and 32 and an appropriate level of guarantee. Compliance with these aspects shall be checked appropriately.

11. Rights of Data Subjects

11.1. Right to Information

Data Subjects have the right of access to their *Personal Data* processed by or on behalf of *Welthungerhilfe*.

11.2. Providing Information

When processing a request for information, the identity of the requestor must be established beyond doubt. If there is reason to doubt their identity, additional information may be requested from the requestor. If the requestor's identity cannot be established beyond reasonable doubt, the information must be refused in writing, with the reason for the refusal provided.

The provision of (or refusal to provide) information is always provided in writing. If the *Data Subject* has submitted the request for information electronically, the information may also be provided electronically. In addition to the *processed Personal Data* of the *Data Subject*, the information should also include the *Recipients* of the data, the purpose of the *Processing*, and all other information required by law, so that the *Data Subject* can personally assess the lawfulness of the Processing. The *Data Protection Officer* shall advise on the necessary scope of the duty to provide information. At the specific request of the *Data Subject*, the data shall be made available in a structured, common, and machine-readable format. The responsible IT unit shall determine the format to be used for this purpose. At the express request of the *Data Subject*, a copy of the *Personal Data* of the *Data Subject* shall be provided.

11.3. Correction

Data Subjects have the right to have their *Personal Data* corrected if it is established to be inaccurate. They may also request the completion of incomplete *Personal Data*. Requests for correction shall be complied with immediately.

11.4. Deletion

Data Subjects have the right to have their *Personal Data* deleted under the following conditions:

- knowledge of the *Personal Data* is no longer necessary to fulfil the purposes for which it was retained;
- the *Data Subject* has withdrawn their *Consent* and there is no other legal basis for the *Processing*;
- the *Data Subject* objects to *Processing* for marketing purposes or invokes a right of objection on the basis of a specific – and justifiable – personal situation;
- *Sensitive Personal Data* are being *processed* and their accuracy cannot be proven; or
- there is another legal obligation to delete the *Personal Data*.

If there is an obligation to delete *Personal Data* that has been previously made public, and to the extent reasonably possible, other *Controllers* responsible for the *Processing* must be informed of the request for deletion by the *Data Subject* with regard to all copies of and links to the data.

11.5. Processing Restriction

The *Data Subject* may request a *Processing Restriction* on their *Personal Data* in the following circumstances:

- the accuracy of the *Personal Data* is in dispute, but only for the period during which the accuracy is being verified by the responsible *Department/Project*;
- the *Processing* is unlawful, but the *Data Subject* refuses to have their *Personal Data* deleted;
- *Welthungerhilfe* no longer needs the *Personal Data* for *processing* purposes, but the *Data Subject* requires the *Personal Data* for the establishment, exercise, or defence of legal claims; or
- the *Data Subject* has objected to the *Processing* based on a special situation, and the responsible *Department/Project* is still examining such objection.

11.6. Response Time

The *Data Subject* shall be informed within one month from the receipt of the request of the substantive measures taken in response to the request.

11.7. Right to Complain

Every *Data Subject* has the right to file a complaint about the *Processing* of their *Personal Data* if they feel their rights have been violated. Complaints may be submitted to the *Data Protection Officer*; the *Data Protection Officer* is independent and autonomous. Complaints may also be submitted to a supervisory authority.

11.8. Advisory Mandate of the Data Protection Officer

The *Data Protection Officer* shall be available to advise on protecting the rights of *Data Subjects*.

12. Requests by *Third Parties* for Information about *Data Subjects*

Should *Third Parties* request information about *Data Subjects*, for example, donors, WHH Employees, or Project Participants supported by Welthungerhilfe, disclosure of information is only permitted if and to the extent that the following cumulatively applies:

- the *Third Parties* requesting the information can demonstrate a legitimate interest in doing so, and
- the information must be provided by law to the requesting *Third Party*, and
- the identity of the *Third Parties* is established beyond doubt.

In case of doubt as to the legitimacy of the request for information, the *Data Protection Officer* shall be consulted before the information is provided. If there is sufficient reason to believe that the disclosure of *Personal Data* to the *Third Parties* would lead to the impairment of essential rights or to a substantial endangerment of the *Data Subject*, the data may only be disclosed with the prior consent of the Association's executive board or the Foundation's management. In making its decision, the Association's executive board / Foundation's management shall consult the *Global Privacy Officer* and the *Data Protection Officer*.

13. Endangering or Violating the Protection of Personal Data ("*Data Breaches*")

13.1. Notification to the Information Security Expert

If a responsible *Department*, *Project*, or *Country Office* identifies weaknesses in its respective information security framework, it shall immediately inform the Information Security Expert and attach a proposal for remedying the weakness. The Information Security Expert shall – if necessary – consult with the relevant IT Department and the relevant *Global* or *Country Privacy Officer*, propose an improvement plan, and monitor its implementation in an advisory and controlling capacity.

13.2. Duty to Inform in case of a material *Data Breach*

The responsible *Department*, *Project*, or *Country Office* shall immediately inform the *Global Privacy Officer* and the *Data Protection Officer* in the following cases:

- in the event of a suspected material breach of the protection of *Personal Data*, in particular if *Third Parties* have gained unlawful access to *Personal Data*. The notification must include all information relevant to clarifying the facts of the case, in particular, the suspected nature of the breach, the *Recipient*, the *Data Subjects*, and the nature and scope of the data involved. The *Global Privacy Officer*, in consultation with the *Data Protection Officer*, shall decide whether to involve the *Data Incident Response Team*;

and

- in the event of inquiries from investigating authorities, supervisory authorities, or legal disputes relating to *Personal Data*; in the latter case, the Legal & Compliance Department shall also be involved.

13.3. Information to Supervisory Authorities and to *Data Subjects*

The *Data Protection Officer* is solely responsible for fulfilling any duty to inform the supervisory authority. The responsible *Department/Project* informs the *Data Subject(s)*, in close alignment with the the *Global Privacy Officer* and the *Data Protection Officer*. In critical cases the Corporate Communications Department must be involved in coordinating communications in a timely manner.

14. Training

All *WHH Employees* are to be appropriately sensitised to the topics of data protection and information security. *WHH Employees* who have ongoing or regular access to *Personal Data*, who process such data (e.g., *WHH Employees* of the Human Resources Department, the Donor Unit, or *Project* staff who process *Project Participants*' data), or who develop or maintain systems for Processing such data shall be trained in an appropriate manner on data protection obligations. The *Global Privacy Officer* shall decide on the form and frequency of such training, in consultation with the *Data Protection Officer*.

15. Audits

15.1. Regular Review of the Level of Data Protection

To ensure an adequate level of data protection, relevant processes shall be regularly reviewed by internal or external bodies under the responsibility of Internal Audit. If a possibility for improvement is identified, corresponding corrective measures shall be identified and implemented in accordance with an action plan.

15.2. Duty to Document and Inform

Audit findings shall be documented in an audit report. The audit report shall be submitted to the *Data Protection Officer* and the *Global Privacy Officer*. Specialists responsible for the audited processes audited shall be appropriately informed of the results.

15.3. Implementation of Improvement Measures

The improvement measures recommended in the audit report must be implemented appropriately. The respective *Department* or *Project* responsible for the processes to be improved is responsible for this. The *Department* or *Project* shall report on the progress and completion of the improvement measures to the responsible *Country Privacy Officer* or *Country Management*. As needed, follow-up audits may be carried out to verify the effective implementation of the recommended improvement measures.

16. Internal Investigations

16.1. Compliance with Data Protection Law

Investigation measures to clarify the facts of a case or to prevent or detect criminal offences or serious breaches of duty in the employment relationship shall be carried out in strict compliance with relevant data protection laws and regulations. In particular, any associated collection and use of data must be necessary to achieve the purposes of the investigation, appropriate, and proportionate to the interests of the *Data Subject*.

16.2. Duty to Inform the *Data Subject*

The Data Subject shall be informed as soon as possible and necessary of the investigation measures taken with respect to them.

16.3. Involvement of the *Data Protection Officer* and Employee Representative

In all forms of internal investigations, the Data Protection Officer must be consulted in advance on the selection and design of the intended measures in order to verify their conformity with applicable data protection law. Likewise, the relevant employee representative body must be appropriately informed or involved in line with applicable law.

17. Accountability

Compliance with the requirements of this *Policy* must be ascertainable at all times. Particular attention must be paid here to the auditability and transparency of measures taken, for example, by means of associated documentation.

18. Updating the *Policy*

This *Policy* shall be regularly reviewed with an eye towards adapting and amending it in the context of further development of data protection law and technological and organisational changes. Changes to this *Policy* must be approved by the *Global Privacy Officer*. They must be documented promptly in writing. WHH Employees must be informed of changed requirements in a prompt and appropriate manner.

19. Complaints, Duty to Report, and Consequences of Violations

19.1. Duty to Report

Anyone with concerns, suspicions or knowledge of incidents regarding violations of this Policy is obligated to immediately report them to the Compliance department at Welthungerhilfe's Head Office via Welthungerhilfe's Reporting Portal (www.welthungerhilfe.org/complaints);  .

The Reporting Portal ensures adequate confidentiality and allows for anonymous reporting.

Any report submitted to management or via national complaint lines to Welthungerhilfe must be passed on by them to the Compliance department via Welthungerhilfe's Reporting Portal.

Nobody who reports suspected violations or submits information regarding such violations with honest intent, needs to fear any disadvantage or other consequences, even if the report later turns out to be unfounded. It is not the responsibility of Employees, Contributors or reporters to conduct investigations, search for evidence, or determine whether a violation of this Policy took place.

Deliberately false accusations will not be tolerated. The failure to report a suspected violation of this Policy constitutes a violation of Welthungerhilfe's Code of Conduct and of this Policy.

Violations of this Policy may result in disciplinary measures, up to and including immediate termination and/or the annulment of cooperation agreements. Welthungerhilfe reserves the right to report criminal offences in compliance with applicable laws.

Additional information is provided in the following documents:

- *Guideline for Reporting Code of Conduct Violations*
- *For Germany: Shop Agreement Whistleblowing System*

Reporting Portal: www.welthungerhilfe.org/complaints

Mathias Mogge
Secretary General / CEO

Christian Monning
Chief Financial Officer