DATENSCHUTZ-POLICY

Genehmigt am:	1. Mai 2024
Genehmigt durch:	Vorstand
Version:	2.1
Erstellt durch:	Legal & Compliance
Prüfzyklus:	2 Jahre
Nächste Gesamtrevision:	2025
Ansprechpartner*in:	Legal & Compliance Compliance@welthungerhilfe.de
Bindend für:	■ Alle Mitarbeitenden der Welthungerhilfe (Deutsche Welthungerhilfe e.V. („**Verein**“) und Stiftung Deutsche Welthungerhilfe („**Stiftung**“), Verein und Stiftung gemeinsam „**Welthungerhilfe**“ oder „**WHH**“)

Es gilt die aktuell gültige Version dieses Dokuments im Intranet unter at www.welthungerhilfe.org/code-of-conduct .

Inhaltsverzeichnis

1. Einleitung

Welthungerhilfe verarbeitet zur erfolgreichen Durchführung ihrer jeweiligen Organisationszwecke *Personenbezogene Daten* in vielfältiger Weise. *Personenbezogene Daten* sind höchstpersönlich. Sie lassen unmittelbare Rückschlüsse auf die dahinterstehenden Personen („***Betroffene Person***“) zu. Eine unsachgemäße *Verarbeitung Personenbezogener Daten* kann daher schwerwiegende Verletzungen höchstpersönlicher Rechte der *Betroffenen Personen* verursachen und sowohl für diese als auch für die *Welthungerhilfe* zu einem schwerwiegenden Schaden führen. Daher nimmt *Welthungerhilfe* den Schutz *Personenbezogener Daten* sehr ernst. Für einen effektiven Schutz bedarf es einer klaren Zuordnung von datenschutzbezogenen Verantwortlichkeiten innerhalb der *Welthungerhilfe*. Diese Datenschutz-Policy („***Policy***“) regelt die Datenschutz-bezogene Zuordnung von Verantwortung und stellt klare Verhaltensregeln für *WHH-Mitarbeitende* auf.

2. Ziele

Das Ziel dieser *Policy* ist es:

- die Grundrechte und Grundfreiheiten von *Betroffenen Personen*, insbesondere ihr Recht auf Schutz *Personenbezogener Daten* zu wahren und durch allgemeine organisatorisch Maßnahmen und Zuordnung von Verantwortlichkeiten ein angemessenes Niveau für den Schutz der von *Welthungerhilfe verarbeiteten Personenbezogenen Daten* zu gewährleisten;
- innerhalb der *Welthungerhilfe* Mindeststandards und einen einheitlichen Rahmen für die Nutzung und den Schutz *Personenbezogener Daten* zu schaffen;
- im Rahmen unserer auf Humanitäre Nothilfe und Entwicklungszusammenarbeit ausgerichteten Tätigkeit entsprechend dem Core Humanitarian Standard für Qualität und Rechenschaftslegung das „do-no-harm-Prinzip“ auch im Bereich des Datenschutzes konsequent umzusetzen;
- die Position der *Welthungerhilfe* als professionelle und glaubwürdige Organisation und das Vertrauen in ihre Tätigkeit zu stärken und Imageschäden von *Welthungerhilfe* und ihren Marken abzuwenden;
- die Einhaltung bestehender rechtlicher, vertraglicher oder anderer Pflichten[1] durch Leitlinien für *WHH-Mitarbeitende* und durch klare Zuordnung von Verantwortlichkeiten zu gewährleisten.

Die *Policy* muss für alle *WHH-Mitarbeitenden* jederzeit leicht zugänglich sein.

3. Geltungsbereich

Die Vorgaben dieser *Policy* gelten für:

a) Vereinsvorstand, Vorstand und Geschäftsführung der Stiftung und alle anderen Mitarbeitenden der *Welthungerhilfe*, unabhängig von Vertragsart (u. a. Angestellte, Aushilfen, Praktikant∗innen, Leiharbeitskräfte), Umfang und Einsatzort des Beschäftigungsverhältnisses (nachfolgend gemeinsam „***WHH-Mitarbeitende***“);
b) Social Business Unternehmen, an denen die *Welthungerhilfe* zu mehr als 50% beteiligt ist.

Die Gebote und Verbote dieser *Policy* gelten für jeglichen Umgang mit *Personenbezogenen Daten*, unabhängig davon, ob dieser elektronisch, in Papierform oder in anderer Form erfolgt.

[1] z.B. Gesetze (DSGVO, Bundesdatenschutzgesetz), Zuwendungsbescheide institutioneller Geber samt Nebenbestimmungen, andere für *Welthungerhilfe* verbindliche Internationale Standards (CHS).

Ebenso bezieht sie alle Arten von *Betroffenen Personen* (Spender∗innen, *WHH-Mitarbeitende*, Lieferant∗innen, Mitarbeitende von Partnerorganisationen, *Projektbeteiligte*, usw.) in ihren Geltungsbereich ein.

Diese *Policy* gilt weltweit als Mindeststandard für alle *WHH-Mitarbeitenden*. Sie ist im Zusammenhang mit dem Verhaltenskodex der *Welthungerhilfe* und den dort genannten Policies und internationalen Standards und Kodizes zu verstehen. Zudem haben *WHH-Mitarbeitende* die an ihrem Einsatzort geltenden Gesetze einzuhalten. Maßgeblich ist dabei die jeweils strengere Vorgabe. Sollten lokale Gesetze Grundsätzen dieser *Policy* widersprechen, wird die zuständige *Landesdirektion* den∗die *Global Privacy Officer* hierüber schriftlich informieren und mit ihm∗ihr eine *Policy*-konforme Lösung abstimmen. Eine Abweichung von dieser *Policy* ist nur mit vorheriger schriftlicher Zustimmung der zuständigen *Landesdirektion* im Benehmen mit dem∗der *Global Privacy Officer* zulässig.

Der Vorstand des Vereins und die Geschäftsführung der Stiftung sind jeweils für die Umsetzung dieser *Policy* in Deutschland und auf globaler Ebene und insgesamt für die Einhaltung des Datenschutzes innerhalb ihrer Organisation verantwortlich.

Die *Landesdirektion* ist jeweils gesondert für die Umsetzung dieser *Policy* in ihren jeweiligen Programmländern verantwortlich. Sie muss sich über die jeweiligen landespezifischen Anforderungen zum Datenschutz informieren und diese angemessen berücksichtigen.

4. Definitionen

Definitionen haben in dieser *Policy* durchgängig denselben Bedeutungskern, unabhängig davon, in welcher Wortform sie verwandt werden[2]; sie sind zur besseren Erkennbarkeit kursiv gesetzt.

4.1. *Anonymisierung*

Anonymisierung ist die *Verarbeitung* von *Personenbezogenen Daten* in einer Weise, die gewährleistet, dass sich die Daten nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen oder *Betroffene Personen* nicht oder nicht mehr – auch nicht indirekt durch Hinzuziehen anderer Informationen – identifiziert werden können.

4.2. *Anwendungsverantwortliche Person*

Für Anwendungen („Software Applications"), die besondere datenschutzrechtliche Betreuung benötigen, ist eine *Anwendungsverantwortliche Person* namentlich zu benennen, die dort, wo die Anwendung operativ verantwortet wird, tätig ist. Die *Anwendungsverantwortliche Person* stellt gemäß Ziff. 6.3.4 sicher, dass datenschutzrelevante Belange bei Entwicklung und Betrieb der Anwendung angemessen berücksichtigt werden und dient als interne Kontaktperson für anwendungsbezogene datenschutzrechtliche Themen.

4.3. *Auftragsverarbeiter∗in*

Auftragsverarbeiter∗in ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die *Personenbezogene Daten* im Auftrag der *Verantwortlichen Person* verarbeitet.

4.4. *Betroffene Person*

Jede natürliche Person, die aufgrund von *Personenbezogenen Daten* identifiziert oder identifizierbar ist, wie zum Beispiel Spender∗innen, *WHH-Mitarbeitende*, Lieferant∗innen, Mitarbeitende von Partnerorganisationen, oder *Projektbeteiligte*.

[2] So z.B. haben die Begriffe „*Verarbeitung*", „*verarbeiten*", „*verarbeitet*", „*verarbeitend*", „Daten*verarbeitung*" denselben definierten Bedeutungskern.

4.5. *Biometrische Daten*

Biometrische Daten sind mit speziellen technischen Verfahren gewonnene *Personenbezogene Daten* zu den physischen, physiologischen oder verhaltenstypischen Markmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

4.6. *Country Privacy Officer*

Jede *Landesdirektion* soll für ihr Landesbüro eine∗n *Country Privacy Officer* ernennen. Die∗der *Country Privacy Officer* nimmt im Verantwortungsbereich des jeweiligen *Landesbüros* die in Ziff. 5.3.1 beschriebenen Aufgaben wahr. Soweit die *Landesdirektion* keine∗n Country Privacy Officer ernennt, bleibt die *Landesdirektion* für diese Aufgaben verantwortlich.

4.7. *Datenpanne*

Eine *Datenpanne* ist jede Verletzung der Sicherheit *Personenbezogener Daten*, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu *Personenbezogenen Daten* führt, die von der *Welthungerhilfe* oder in deren Auftrag verarbeitet werden.

4.8. *Data Incident Response Team*

Im *Head Office* wird ein *Data Incident Response Team* eingerichtet, das zumindest mit den folgenden Funktionen besetzt ist: *Global Privacy Officer*, Head of IT, Information Security and Data Protection Expert. Die∗der *Global Privacy Officer* kann das *Data Incident Response Team* bei Bedarf je nach Sachlage erweitern. Sollte eine schwerwiegende *Datenpanne* in einem *Landesbüro* auftreten, muss die∗der jeweilige Country Privacy Officer des *Landesbüros* zum *Data Incident Response Team* hinzugezogen werden. Aufgabe des *Data Incident Response Teams* ist es, bei vermuteten oder festgestellten schwerwiegenden *Datenpannen* angemessene Maßnahmen festzulegen, welche den Schaden der *Datenpanne* minimieren, die *Datenpanne* unverzüglich abstellen und beheben, angemessen *Betroffene Personen* und/oder Aufsichtsbehörden informieren und zukünftige *Datenpannen* verhindern.

4.9. *Datenschutzbeauftragte∗r*

Die∗der *Datenschutzbeauftragte* ist eine nach zwingendem anwendbarem Recht einzurichtende Funktion des *Head Office* oder eines *Landesbüros*, welche bei der Sicherstellung der Einhaltung datenschutzrechtlicher Bestimmungen unterstützt.

4.10. *Datenschutz-Grundverordnung („DSGVO“)*

Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) in der jeweils geltenden Version (ABl. L 119, 04.05.2016; ber. ABl. L 127, 23.05.2018).

4.11. *Dritte*

Dritte sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, außer der *Betroffenen Person*, der *Verantwortlichen Person*, dem∗der *Auftragsverarbeiter∗in* und den Personen, die unter der unmittelbaren Verantwortung der *Verantwortlichen Person* oder des∗der *Auftragsverarbeiters∗Auftragsverarbeiterin* befugt sind, die *Personenbezogenen Daten* zu verarbeiten.

4.12. *Einschränkung*

Einschränkung der *Verarbeitung* ist die Markierung gespeicherter *Personenbezogener Daten* mit dem Ziel, ihre künftige *Verarbeitung* einzuschränken.

4.13. *Einwilligung*

Eine *Einwilligung* der *Betroffenen Person* ist jede freiwillig für einen bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung

oder einer sonstigen eindeutigen bestätigenden Handlung, durch welche die *Betroffene Person* zu verstehen gibt, dass sie mit der *Verarbeitung* der sie betreffenden *Personenbezogenen Daten* einverstanden ist.

4.14. *Empfangende Person*

Empfangende Person[3] ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der *Personenbezogene Daten* offengelegt werden, unabhängig davon, ob es sich bei ihr um *Dritte* handelt oder nicht.

4.15. *Fachabteilung (Unit)*

Eine permanente und selbständige funktionale Einheit des *Head Office* oder eines *Landesbüros*, die im *entsprechenden* Organigramm des *Head Office/Landesbüros* abgebildet ist (z.B. Finanzen, Personal, Logistik, Innenrevision, oder Kommunikation).

4.16. *Genetische Daten*

Genetische Daten sind *Personenbezogene Daten* zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person geben und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

4.17. *Global Privacy Officer*

Der Vereinsvorstand ernennt im Benehmen mit der Geschäftsführung der Stiftung für die *Welthungerhilfe* eine∗n *Global Privacy Officer*. Die∗der *Global Privacy Officer* berichtet direkt an den Vorstand; für Belange, welche nur die Stiftung betreffen, berichtet sie∗er unmittelbar an die Geschäftsführung der Stiftung. Sie∗er übt ihre∗seine in Ziff. 5.3.2 beschriebenen Aufgaben weisungsfrei und unter Anwendung ihres∗seines Fachwissens aus.

4.18. *Internationale Organisation*

Eine *Internationale Organisation* ist eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf Grundlage einer solchen Übereinkunft geschaffen wurde.

4.19. *Head Office*

Die Organisation der *Welthungerhilfe* an den Standorten in Bonn und Berlin.

4.20. *Landesbüro*

Das im Ausland eingerichtete und meist akkreditierte Büro, das unter anderem die Vorbereitung und Durchführung von diesem Land zugeordneten Programmen und *Projekten* koordiniert und/oder verantwortet.

4.21. *Landesdirektion*

Die *Landesdirektion* ist die für ein bestimmtes Land zuständige exekutive Leitungsfunktion. In Deutschland ist dies der Vorstand / die Geschäftsführung der WHH. In den Programmländern sind dies die jeweiligen Landesdirektor∗innen. Sind in einem Land mehrere Landesdirektor∗innen ernannt, gelten sie gemeinsam als *Landesdirektion*. Sofern in einem Land *Projekte* ohne die Errichtung eines *Landesbüros* durchgeführt werden, ist im Rahmen der Planung dieser *Projekte* festzulegen, wer für diese *Projekte* die Aufgaben und Verantwortlichkeiten der *Landesdirektion* unter dieser *Policy* übernimmt.

[3] Empfänger i.S. von Art.4 Nr. 9 *DSGVO*.

4.22. *Personenbezogene Daten*

Personenbezogene Daten sind alle Informationen, die sich auf eine *Betroffene Person* beziehen, wie z.B. Spender∗innen-Daten, Daten von Umsetzungspartnern oder *Projektbeteiligten* oder Personaldaten von *WHH-Mitarbeitenden*. Es genügt, wenn die jeweilige Information mit dem Namen der *Betroffenen Person* verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann, auch wenn die Information mit einem Zusatzwissen erst verknüpft werden muss.[4]

4.23. *Policy*

Diese Datenschutz-Policy in ihrer jeweils aktuellen Fassung.

4.24. *Projekt*

Eine zeitlich befristete Organisationseinheit, die mit eigenem Budget ausgestattet ist und zum Zweck der Umsetzung von bestimmten Maßnahmen der humanitären Nothilfe oder der Entwicklungszusammenarbeit in einem Programmland errichtet wurde und normalerweise von einem Head of Project geführt wird.

4.25. *Projektbeteiligte*

Projektbeteiligte sind Zielgruppen von Programmen und *Projekten*, die von der *Welthungerhilfe* oder ihren Partnerorganisationen durchgeführt werden, sowie Mitglieder der Gemeinschaften, in denen die *Welthungerhilfe* und ihre Partnerorganisationen tätig sind als auch alle Personen, die aktiv an den Programmen oder *Projekten* der *Welthungerhilfe* oder ihrer Partnerorganisationen beteiligt ist und keine *WHH-Mitarbeitende* oder Mitarbeitende einer Partnerorganisation sind.

4.26. *Profiling*

Profiling bezeichnet jede Art der automatisierten *Verarbeitung Personenbezogener Daten*, die darin besteht, dass diese *Personenbezogenen* Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, körperlichen Zustand, Ernährungszustand, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

4.27. *Pseudonymisierung*

Pseudonymisierung ist die *Verarbeitung Personenbezogener Daten* in einer Weise, dass die *Personenbezogenen Daten* ohne Hinzuziehung zusätzlicher Informationen nicht mehr bestimmten *Betroffenen Personen* zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die *Personenbezogenen Daten* nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

[4] Beispielsweise lässt der Name eines Ansprechpartners ebenso einen Rückschluss auf eine natürliche Person zu, wie seine E-Mail-Adresse oder die IP-Adresse des Besuchers einer Website. Auch Fotos, Video- oder Tonaufnahmen können *Personenbezogene Daten* darstellen.

4.28. *Sensible Personenbezogene Daten*

Sensible Personenbezogene Daten[5] sind Informationen, aus denen die ethnische oder andere Herkunft[6], politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder eine Gewerkschaftszugehörigkeit hervorgehen kann sowie *genetische Daten*, *biometrische Daten* zur eindeutigen Identifikation einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung einer natürlichen Person.

4.29. *Stiftung*

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

4.30. *Verarbeitung*

Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit *Personenbezogenen Daten*, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die *Einschränkung*, das Löschen oder die Vernichtung. So ist z.B. bereits die Erhebung von *Personenbezogenen Daten* bei *Projektbeteiligten* eine *Verarbeitung*, aber auch das bloße Zeigen von *Personenbezogenen Daten* auf einem Tablet ist eine Weitergabe und damit eine *Verarbeitung*.

4.31. *Verein*

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

4.32. *Verantwortliche Person*

Verantwortliche Person[7] ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der *Verarbeitung* von *Personenbezogenen Daten* entscheidet. *Verantwortliche Person* des *Vereins* ist der Deutsche Welthungerhilfe e.V.; *Verantwortliche Person* der *Stiftung* ist die Stiftung Deutsche Welthungerhilfe.

4.33. *Welthungerhilfe bzw. WHH*

Der Deutsche Welthungerhilfe e.V. und die Stiftung Deutsche Welthungerhilfe, soweit sich diese *Policy* kumulativ oder alternativ auf beide bezieht.

4.34. *WHH-Mitarbeitende*

Vereinsvorstand, Vorstand und Geschäftsführung der Stiftung und alle anderen Mitarbeitenden der *Welthungerhilfe*, unabhängig von Vertragsart (u. a. Angestellte, Aushilfen, Praktikant*innen, Leiharbeitskräfte), Umfang und Einsatzort des Beschäftigungsverhältnisses.

---

[5] Die DSGVO verwendet den Begriff „Besondere Kategorien Personenbezogener Daten“. Der in der *Policy* aus Verständlichkeitsgründen verwandte Begriff der „*Sensiblen Personenbezogenen Daten*“ hat dieselbe Bedeutung.

[6] Die *Policy* verwendet bewusst nicht den in der DSGVO verwandten Begriff der „rassischen“ Herkunft um klarzustellen, dass *Welthungerhilfe* Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, ablehnt. Eine Beschränkung der gesetzlichen Definition ist damit nicht beabsichtigt.

[7] „Verantwortlicher“ i.S. von Art. 4 Nr. 7 *DSGVO*.

5. Datenschutz-Aufbauorganisation

5.1. Allgemeine Organisation

Die datenschutzbezogenen Verantwortlichkeiten liegen übergeordnet global beim Vorstand und für jedes Land bei der *Landesdirektion*. Bei Wahrnehmung ihrer jeweiligen Aufgaben werden der Vorstand und die *Landesdirektionen* von der∗dem *Global Privacy Officer* bzw. der∗dem *Country Privacy Officer* unterstützt.

5.2. Lokale Gesamtverantwortung

Die *Landesdirektion* ist im Verantwortungsbereich des jeweiligen *Landesbüros* für die Einhaltung datenschutzrechtlicher Vorgaben verantwortlich. Zudem hat sie dafür Sorge zu tragen, dass Führungskräfte, *WHH-Mitarbeitende* und etwaige *Dritte* (einschließlich Partnerorganisationen), die *Personenbezogenen Daten* im Verantwortungsbereich des *Landesbüros verarbeiten*, entsprechend der *DSGVO* und lokalen Anforderungen informiert und, soweit erforderlich, angemessen geschult werden.

5.3. Festlegung der Verantwortlichkeiten

Die *Landesdirektion* muss innerhalb ihres Verantwortungsbereichs die Aufgaben und Verantwortlichkeiten im Umgang mit *Personenbezogenen Daten* eindeutig festlegen, regelmäßig kontrollieren und dokumentieren. Zu ihrer Unterstützung soll sie eine∗n *Country Privacy Officer* ernennen. Soweit sie keine∗n *Country Privacy Officer* ernennt, bleibt die *Landesdirektion* für dessen Aufgaben verantwortlich.

Bei der Festlegung der Aufgaben und Verantwortlichkeiten im Umgang mit *Personenbezogenen Daten* sind folgende Maßgaben zu berücksichtigen:

5.3.1. Country Privacy Officer

Die∗der *Country Privacy Officer* ist im Verantwortungsbereich des jeweiligen *Landesbüros* dafür zuständig, die Einhaltung datenschutzrechtlicher Vorgaben zu unterstützen. Zudem ist sie∗er für die Koordination datenschutzrechtlicher Themen und dieser *Policy* in dem jeweiligen Land zuständig. Sie∗er dient auch als Ansprechperson für das *Head Office* und die *Global Privacy Officers* und stellt ihnen Informationen zu datenschutzrelevanten Belangen des *Landesbüros* zur Verfügung. Soweit gesetzlich vorgesehen, ist für das *Landesbüro* auch ein∗e *Datenschutzbeauftragte∗r* zu bestellen; diese∗r kann[8] in Personalunion die Aufgaben der∗des *Country Privacy Officer* ausüben. Die∗der *Global Privacy Officer* ist den *Country Privacy Officers* fachlich vorgesetzt; disziplinarisch vorgesetzt ist die *Landesdirektion*. Disziplinarische Maßnahmen gegen *Country Privacy Officers* bedürfen der vorherigen Zustimmung der∗des *Global Privacy Officer*.

5.3.2. Global Privacy Officer

Die∗der *Global Privacy Officer* nimmt die Berichte der∗des *Datenschutzbeauftragten* für den Vereinsvorstand bzw. die Geschäftsführung der Stiftung entgegen und leitet diese jeweils entsprechend weiter. Zudem unterstützt sie∗er den Vereinsvorstand, die Geschäftsführung der Stiftung, die *Landesbüros* und die dortigen *Country Privacy Officers* bei ihren jeweiligen Aufgaben, insbesondere bei der Umsetzung und Auslegung WHH-weit geltender datenschutzrechtlicher Bestimmungen, unter anderem durch Vorgabe von Prozessen und Mustern. Darüber hinaus koordiniert die∗der *Global Privacy Officer* datenschutzrechtliche Themen mit WHH-weiter Relevanz. Die∗der *Global Privacy Officer* ist den *Country Privacy Officers* fachlich vorgesetzt.

[8] Soweit gesetzlich zulässig.

5.3.3. Datenschutzbeauftragte*r

Das *Welthungerhilfe Head Office* hat zusätzlich eine*n gesetzlichen *Datenschutzbeauftragte*n* bestellt. Sie*er ist erreichbar unter folgenden Kontaktdaten:

- Email: Datenschutz@welthungerhilfe.de,
- Postalisch: Deutsche Welthungerhilfe e.V. „Datenschutzbeauftragte*r", Friedrich-Ebert-Str. 1, 53173 Bonn-Bad Godesberg, Deutschland

Die*der *Datenschutzbeauftragte* überwacht die Einhaltung der *DSGVO* sowie anderer gesetzlicher oder untergesetzlicher Vorgaben, und der Vorgaben dieser und anderer Policies der *Welthungerhilfe* zum Datenschutz. Die*der *Datenschutzbeauftragte* berät und unterrichtet den Vereinsvorstand und die Geschäftsführung der Stiftung hinsichtlich bestehender Datenschutzpflichten und ist zuständig bei der Kommunikation mit Aufsichtsbehörden. Ausgewählte Prozesse werden stichprobenartig, risikoorientiert und in angemessenen Zeitabständen durch die*den *Datenschutzbeauftragte*n* auf ihre Datenschutzkonformität hin kontrolliert.

Die*der *Datenschutzbeauftragte* nimmt ihre*seine Aufgaben weisungsfrei und unter Anwendung ihres*seines Fachwissens wahr. Sie*er berichtet fachlich unmittelbar an die*den *Global Privacy Officer*. Bei Dringlichkeit, Nicht-Erreichbarkeit der*des *Global Privacy Officer* oder gebotener direkter Berichterstattung an den Vereinsvorstand oder die Geschäftsführung der Stiftung kann die*der *Datenschutzbeauftragte* auch unmittelbar den Vereinsvorstand bzw. die Geschäftsführung der Stiftung informieren, allerdings immer mit Kopie an die*den *Global Privacy Officer*, sofern dem keine zwingenden Gründe entgegenstehen.

Alle Fachabteilungen und alle *WHH-Mitarbeitenden* haben die*den *Datenschutzbeauftragte*n* bei der Erfüllung ihrer*seiner Aufgaben zu unterstützen.

6. Allgemeine Prinzipien und Ablauforganisation

6.1. Informationssicherheitskonzept: Verfügbarkeit, Vertraulichkeit und Integrität von Daten

6.1.1. Allgemeines Informationssicherheitskonzept

Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität von Informationen wird auf Basis der Policy Informationssicherheit ein allgemeines Sicherheitskonzept in Abhängigkeit der Schutzbedarfsfeststellung und Risikoanalyse erstellt, das für alle Verfahren der *Verarbeitung* von Informationen und damit auch für die *Verarbeitung Personenbezogener Daten* verbindlich ist. Hierin ist insbesondere der Stand der Technik zu berücksichtigen.

Das Sicherheitskonzept ist hinsichtlich der Wirksamkeit der dort vorgesehenen technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen und zu bewerten. Für den Umgang mit Informationen ist ein Klassifizierungssystem aufzustellen. Alle *WHH-Mitarbeitenden* sind bezüglich des sorgfältigen Umgangs mit Informationen, insbesondere vertraulichen und sensiblen Informationen, einschließlich *Personenbezogenen Daten*, angemessen, auch in Form von Schulungen, zu sensibilisieren. Einzelheiten hierzu regelt die Policy Informationssicherheit (Information Security Policy).

6.1.2. Risikobewertung zur Verarbeitung Personenbezogener Daten

In Abhängigkeit von der Art, des Umfangs, der Umstände und der Zwecke der *Verarbeitung* sowie der Eintrittswahrscheinlichkeit einer *Datenpanne* muss die mit der *Verarbeitung* der *Personenbezogenen Daten* befasste *Fachabteilung* den Schutzbedarf der *Verarbeitung* selbst und der darin verarbeiteten Daten mit Blick auf die Folgen einer möglichen *Datenpanne* für die *Betroffene Personen* ermitteln (vgl. hierzu auch Ziff. 6.3.2 (Allgemeine Risikobewertung) und Ziff. 6.3.3 (Datenschutz-Folgenabschätzung)). Hierzu können die *Country Privacy Officer*, die*der *Global Privacy Officer* oder die*der *Datenschutzbeauftragte* zu Rate gezogen werden.

6.1.3. Verpflichtung auf das Datengeheimnis

WHH-Mitarbeitenden ist es untersagt, *Personenbezogene Daten* unbefugt zu *verarbeiten*. Sie sind vor Aufnahme ihrer Tätigkeit auf einen vertraulichen Umgang mit *Personenbezogenen Daten* zu verpflichten. Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars. *WHH-Mitarbeitende* mit besonderen Geheimhaltungsverpflichtungen werden ergänzend darauf schriftlich verpflichtet.

6.1.4. Besondere Sicherheitsvorkehrungen bei Verarbeitung Personenbezogener Daten

Die Vorgaben der Policy Informationssicherheit sind zu befolgen. Zugriff auf *Personenbezogene Daten* sollen nur diejenigen Personen erhalten, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen („**Need-to-know-Prinzip**"). Zugriffsberechtigungen müssen genau und vollständig festgelegt und dokumentiert sein, regelmäßig überprüft und gegebenenfalls aktualisiert werden. Übertragungen von *Personenbezogenen Daten* durch öffentliche Netze sind nach Möglichkeit zu verschlüsseln. Eine Verschlüsselung hat zwingend zu erfolgen, falls der Schutzbedarf der *Personenbezogenen Daten* dies erfordert.

Zu unterschiedlichen Zwecken erhobene *Personenbezogene Daten* sind getrennt voneinander zu *verarbeiten*. Die Trennung von Daten ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen.

Es ist zu gewährleisten, dass Dienstleister*innen nicht unbefugt auf *Personenbezogene Daten* zugreifen können. Fernwartungszugänge sind nur im Einzelfall zu gewähren und müssen dem Prinzip der minimalen Rechtevergabe folgen. Fernwartungsaktivitäten sind nach Möglichkeit aufzuzeichnen oder zu protokollieren.

6.2. Verzeichnis von Verarbeitungstätigkeiten

6.2.1. Pflicht, ein Verzeichnis zu führen

Das *Head Office* und jedes *Landesbüro* der *Welthungerhilfe* haben jeweils ein Verzeichnis über alle jeweils von ihnen durchgeführten oder veranlassten *Verarbeitungen Personenbezogener Daten* zu führen. Jede *Fachabteilung*/jedes *Projekt* muss eine Person benennen, die alle notwendigen Informationen zu den Verfahren der jeweiligen Abteilung nach den gesetzlichen Anforderungen und nach dieser *Policy* dokumentiert und pflegt; die*der *Datenschutzbeauftragte* oder die (*Global/Country*) *Privacy Officers* können zur Beratung hinzugezogen werden.

6.2.2. Konsolidiertes Verzeichnis

Die Verzeichnisse der *Landesbüros* und des *Head Office* sind in angemessener Weise in einem Gesamtverzeichnis zu konsolidieren und in regelmäßigen Abständen auf Richtigkeit, Vollständigkeit und Konsistenz zu überprüfen.

6.2.3. Vorlage

Die *Welthungerhilfe* stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung. Zuständig hierfür ist die*der *Datenschutzbeauftragte* in Abstimmung mit der*dem *Global Privacy Officer*.

6.3. Allgemeine Organisatorische Maßnahmen

6.3.1. Verantwortlichkeit im Umgang mit Personenbezogenen Daten

Die Aufgaben und Verantwortlichkeiten im Umgang mit *Personenbezogenen Daten* sind eindeutig festzulegen und deren Umsetzung regelmäßig zu kontrollieren und zu dokumentieren.

6.3.2. Allgemeine Risikobewertung

Jedes *Landesbüro* muss die datenschutzrechtlichen Risiken einschließlich damit verbundener Reputationsrisiken regelmäßig erheben und hinsichtlich möglicher Auswirkungen auf die

Geschäftsabläufe bewerten. Die Ergebnisse dieser Risikoanalyse müssen dokumentiert und - sofern für die *Welthungerhilfe* wesentlich - in das zentrale Risikomanagement einfließen.

6.3.3. Datenschutz-Folgenabschätzung

Jede *Fachabteilung* und jedes *Projekt*, die/das in eigener Verantwortung *Personenbezogene Daten* verarbeitet, deren *Verarbeitung* ein hohes Risiko für Rechte und Freiheiten von *Betroffenen Personen* auslösen kann, muss vor Beginn der *Verarbeitung* eine Datenschutz-Folgenabschätzung durchführen. Dies gilt insbesondere für die *Verarbeitung* von *Personenbezogenen Daten* vulnerabler *Projektbeteiligter*. Ein solches hohes Risiko liegt zum Beispiel vor, wenn standardmäßig eine große Menge von *Personenbezogenen Daten* verarbeitet werden soll, eine umfangreiche *Verarbeitung Sensibler Personenbezogener Daten* oder eine umfassende und systematische Bewertung von persönlichen Aspekten von *Betroffenen Personen* erfolgen soll oder in sonstiger Weise durch die *Verarbeitung*svorgänge ein sehr hohes Risiko für die *Betroffene Person* zu erwarten ist. Ebenso ist eine Datenschutz-Folgenabschätzung durchzuführen, wenn neue Technologien zur Daten*verarbeitung* eingeführt werden sollen. Die Datenschutz-Folgenabschätzung muss schriftlich dokumentiert werden und zumindest folgenden Inhalt haben:

- eine systematische Beschreibung der geplanten *Verarbeitung*svorgänge und der Zwecke der *Verarbeitung*, gegebenenfalls einschließlich der von der *Verantwortlichen Person* verfolgten berechtigten Interessen;
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der *Verarbeitung*svorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der *Betroffenen Personen* und die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz *Personenbezogener Daten* sichergestellt werden soll.

Die*der *Datenschutzbeauftragte* berät die *Fachabteilungen/Projekte* bei der Durchführung der Datenschutz-Folgenabschätzung sowie bezüglich der Frage, wann *Verarbeitungen* ein hohes Risiko für *Betroffene Personen* beinhalten können.

6.3.4. Anwendungsverantwortliche Person für datenschutz-intensive Anwendungen

Für Anwendungen, die besondere datenschutzrechtliche Betreuung benötigen, ist eine *Anwendungsverantwortliche Person* namentlich zu benennen, die dort, wo die Anwendung operativ geführt wird, tätig ist. Die *Anwendungsverantwortliche Person* hat sicherzustellen, dass datenschutzrelevante Belange bei Entwicklung (vgl. Ziff. 6.3.5) und Betrieb der Anwendung angemessen berücksichtigt werden. Sie dient zudem als interne Kontaktperson für anwendungsbezogene datenschutzrechtliche Themen. Solche Anwendungen sind in der Regel (i) Webseiten und Apps, (ii) IT-Systeme, in denen in großer Menge *Personenbezogene Daten* verarbeitet werden (Spender*innen- und Userverwaltung, Business Information, Hinweisgebersysteme), (iii) die Verwaltung von *Einwilligungen* (Opt-Ins) und Widersprüchen sowie (iv) die *Verarbeitung* von Daten von *WHH-Mitarbeitenden* oder *Projektbeteiligten*, Gesundheitsdaten, Bank-/Kreditkartendaten oder von anderen *Sensiblen Personenbezogener Daten*.

6.3.5. Entwicklung, Beschaffung und Verwendung von Geschäftsmodellen und IT-Systemen zur Verarbeitung Personenbezogener Daten

Bei der Entwicklung von Geschäftsmodellen und IT-Systemen, die *Personenbezogene Daten verarbeiten*, sind die rechtlichen und technischen Anforderungen des Datenschutzes bereits in der Konzeption zu beachten (u. a. „**Privacy by Design**“; „**Privacy by Default**“). Dies beinhaltet insbesondere angemessene aktuelle technische Anforderungen, technische und organisatorische Maßnahmen, datenschutzfreundliche Voreinstellungen, die Trennung und Verschlüsselung von Daten sowie die Erstellung und Einhaltung eines Konzeptes für die Aufbewahrung,

Pflege und Löschung der Daten. Der Grundsatz der Datensparsamkeit (vgl. Ziff. 7.2) ist zwingend zu berücksichtigen.

Bei der Auswahl und Gestaltung von Daten*verarbeitung*ssystemen ist Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Daten*verarbeitung*ssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern, so insbesondere den Grundsatz der Datensparsamkeit. Die Verwendung und Voreinstellungen von eingesetzten Daten*verarbeitung*ssystemen sind so zu gestalten, dass sie den Grundsatz der Datensparsamkeit berücksichtigen.

7. Allgemeiner Umgang mit *Personenbezogenen Daten*

7.1. Verarbeitung nur aufgrund gesetzlicher Erlaubnisnorm

Die *Verarbeitung Personenbezogener Daten* ist grundsätzlich verboten, es sei denn, eine gesetzliche Norm erlaubt explizit die *Verarbeitung*. *Personenbezogene Daten* dürfen nach der *DSGVO* grundsätzlich verarbeitet werden, wenn und soweit:

- dies für die Durchführung eines bestehenden Vertragsverhältnis mit der *Betroffenen Person* erforderlich ist.
  Beispiel: Die Speicherung und Verwendung erforderlicher *Personenbezogener Daten* im Rahmen eines Beratungsvertrages oder eines Beschäftigungsverhältnisses.
- dies im Zuge vorvertraglicher Maßnahmen auf Anfrage der *Betroffenen Person* sowie der Vertragsabwicklung mit der *Betroffenen Person* erforderlich ist.
  Beispiel: Interessierte Spender*innen fordern Informationsmaterialien oder Nachweise über die generelle Spendenverwendung an und entscheiden sich schließlich zu spenden. Die erforderlichen Daten zur Zusendung des Informationsmaterials sowie zur Abwicklung der Spende (z.B. Daten zur Ausstellung und Zusendung der Spendenbescheinigung) dürfen verarbeitet werden.
- die *Betroffene Person* freiwillig und informiert *eingewilligt* hat.
  Beispiel: Die *Betroffene Person* meldet sich freiwillig zum Erhalt eines Newsletters an oder ein *Projektbeteiligter* willigt in die *Verarbeitung* ihrer Daten bei der Verwendung von Cash Cards ein.
- eine rechtliche Verpflichtung besteht, der die *Welthungerhilfe* unterliegt.
  Beispiel: Gesetzliche Aufbewahrungsfristen nach Handelsgesetzbuch (HGB) oder Abgabenordnung (AO).
- die *Verarbeitung Personenbezogener Daten* erforderlich ist, um ein lebenswichtiges Interesse der *Betroffenen Person* oder einer anderen natürlichen Person zu schützen.
  Beispiel: Die *Verarbeitung* für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder von Menschen verursachten Katastrophen.
- berechtigte Interessen der *Welthungerhilfe* an der *Verarbeitung* bestehen und gleichzeitig die Interessen oder Grundrechte *Betroffener Personen* nicht überwiegen, insbesondere wenn es sich um ein Kind handelt. Daten*verarbeitungen* unter Berufung auf ein berechtigtes Interesse sollten jedoch nicht ohne vorherige, zu dokumentierende Beratung durch die*den *Datenschutzbeauftragte*n*, den*die *Country* oder *Global Privacy Officer* vorgenommen werden.
  Beispiel: Die Nutzung der postalischen Anschrift aktiver Spender*innen zur Aussendung von Werbeschreiben.

7.2. Grundsatz der Datensparsamkeit

Die *Verarbeitung* von *Personenbezogenen Daten* ist an dem Ziel auszurichten, so wenige Daten wie möglich von *Betroffenen Personen* zu verarbeiten. *Personenbezogene Daten* dürfen nur soweit *verarbeitet* werden, als dies zur Erreichung des legitimen *Verarbeitung*szwecks

erforderlich ist. Insbesondere sind *Personenbezogene Daten* zu *anonymisieren* oder zu *pseudonymisieren*, soweit dies nach dem Verwendungszweck möglich ist. Beispielsweise wird es im Rahmen einer statistischen Auswertung von Daten meist nicht erforderlich sein, Namen der *Betroffenen Personen* zu kennen und zu verwenden. Vielmehr kann diese Information durch einen Zufallswert ersetzt werden, der eine Unterscheidbarkeit der zugrunde liegenden Information ebenfalls gewährleisten kann.

7.3. Bestimmung eines eindeutigen Verarbeitungszwecks

Personenbezogene Daten dürfen nur für einen zuvor festgelegten, eindeutigen und legitimen Zweck verarbeitet werden. Eine Daten*verarbeitung* ohne legitimen Zweck, so beispielsweise die Speicherung von Daten auf bloßen Vorrat, ist unzulässig.

7.4. Änderung des Verarbeitungszwecks

Die Änderung des Zwecks, der einer Daten*verarbeitung* ursprünglich zugrunde gelegt wurde, ist bei einer zuvor erfolgten *Einwilligung* durch die *Betroffene Person* nur zulässig, wenn der Zweck der Weiter*verarbeitung* mit dem von der ursprünglichen *Einwilligung* abgedeckten Zweck vereinbar ist. Hierbei sind insbesondere die vernünftigen Erwartungen der *Betroffenen Person* hinsichtlich einer solchen Weiter*verarbeitung* gegenüber der *Welthungerhilfe*, die Art der verwendeten Daten, die Folgen für die *Betroffene Person* sowie Möglichkeiten einer Verschlüsselung oder *Pseudonymisierung* zu berücksichtigen. Die *Betroffene Person* ist über die Änderung des *Verarbeitungs*zwecks umfassend zu informieren. Der∗die *Datenschutzbeauftragte* berät über den angemessenen Umfang der Informationspflicht.

7.5. Angemessene Information von Betroffenen Personen

Betroffene Personen sind bei der Erhebung ihrer *Personenbezogenen Daten* angemessen über den Umgang mit ihren Daten zu informieren. Die Information muss den *Verarbeitungs*zweck, die Identität der verantwortlichen Stelle, die *Empfangende Person* der *Personenbezogenen Daten* sowie alle erforderlichen Informationen enthalten, um eine faire und transparente *Verarbeitung* zu gewährleisten. Die Information ist in einer verständlichen und leicht zugänglichen Form sowie einer möglichst einfachen Sprache zu verfassen. In Zweifelsfällen stimmen die (*Global/Country*) *Privacy Officers* mit der∗dem *Datenschutzbeauftragten* den angemessenen Umfang der Informationspflicht ab und dokumentieren das Ergebnis dieser Abstimmung.

7.6. Datenerhebung bei Dritten/Nachträgliche Änderung des Verarbeitungszwecks

Werden *Personenbezogene Daten* nicht bei der *Betroffenen Person* erhoben, sondern werden beispielsweise bei einem anderen Unternehmen beschafft, ist die *Betroffene Person* nachträglich und umfassend über den Umgang mit ihren Daten zu informieren. Der∗die *Datenschutzbeauftragte* berät über den angemessenen Umfang der Informationspflicht.

7.7. Datenintegrität

Die *Welthungerhilfe* muss – soweit mit angemessenem Aufwand möglich - sicherstellen, dass verarbeitete *Personenbezogenen Daten* sachlich richtig und, wenn nötig, auf dem neusten Stand sind. Der Umfang der Daten*verarbeitung* muss hinsichtlich des festgelegten *Verarbeitungs*zwecks erforderlich und relevant sein. Die jeweilige *Fachabteilung/Projekt* muss die Umsetzung durch die Etablierung entsprechender Prozesse sicherstellen und Datenbestände regelmäßig in angemessener Weise auf ihre Richtigkeit, Erforderlichkeit und Aktualität hin überprüfen.

8. Sensible Personenbezogene Daten

8.1. Besondere Verarbeitungsvoraussetzung

Sensible Personenbezogene Daten (vgl. Ziff. **Error! Reference source not found.**) dürfen grundsätzlich nur mit *Einwilligung* der *Betroffenen Person* oder ausnahmsweise aufgrund einer besonderen, expliziten gesetzlichen Erlaubnis *verarbeitet* werden. Ferner sind bei jeder *Verarbeitung* zusätzliche technische und organisatorische Maßnahmen (z. B. Verschlüsselung beim Transport, minimale Rechtevergabe) zum Schutz *Sensibler Personenbezogener Daten* zu ergreifen. Der Widerruf der *Einwilligung* durch eine *Betroffene Person* ist möglich und zu beachten.

8.2. Anzeigepflicht

Beabsichtigt eine *Fachabteilung*, ein *Projekt* oder ein *Landesbüro*, *Sensible Personenbezogene Daten* zu verarbeiten, muss die zuständige *Fachabteilung*, das *Projekt* oder das *Landesbüro* die beabsichtigte *Verarbeitung* unter Einbindung der*des zuständigen *Country Privacy Officer* der*dem *Global Privacy Officer* und der*dem *Datenschutzbeauftragten* schriftlich und rechtzeitig im Voraus (wenn möglich, bereits bei Vorbereitung des Projektantrags) anzeigen. Hierbei ist die Notwendigkeit der *Verarbeitung* zu begründen; ebenso sind die bei der *Verarbeitung* anzuwendenden besonderen technischen und organisatorischen Maßnahmen zum Schutz von *Sensiblen Personenbezogenen Daten* transparent darzulegen.

9. Datenübermittlung

9.1. Besondere Erlaubnis

Die Übermittlung von *Personenbezogenen Daten* an *Dritte* ist nur aufgrund gesetzlicher Erlaubnis oder mit der *Einwilligung* der *Betroffenen Person* zulässig.

9.2. Übermittlung in Länder außerhalb der Europäischen Union/EWR/an internationale Organisationen

Befindet sich die *Empfangende Person Personenbezogener Daten* außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums oder ist die *Empfangende Person* eine *Internationale Organisation*, bedarf es zusätzlicher Maßnahmen zur Wahrung von Rechten und Interessen der *Betroffenen Personen*. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist oder - beispielsweise über besondere Vertragsklauseln - nicht hergestellt werden kann.

10. Externe Dienstleistende als *Auftragsverarbeiter*in*

10.1. Zugriff durch externe Dienstleistende auf Personenbezogene Daten

Sofern externe Dienstleistende Zugriff auf *Sensible Personenbezogene Daten* erhalten sollen, ist die*der *Datenschutzbeauftragte* vorab zu informieren. Hierbei sind auch die besonderen Maßgaben nach Ziffer 6.1.4 dieser *Policy* im Falle von Fernwartungen zu beachten.

10.2. Pflicht zur sorgfältigen Auswahl

Dienstleistende mit einem möglichen Zugriff auf *Personenbezogene Daten* sind vor der Auftragserteilung sorgfältig auszuwählen. Die Auswahl ist zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:

- Fachliche Eignung der Dienstleistenden für den konkreten Datenumgang
- Von den Dienstleistenden zugesicherte technisch-organisatorische Sicherheitsmaßnahmen
- Erfahrung der Dienstleistenden im Markt

- Sonstige Aspekte, die auf eine Zuverlässigkeit der Dienstleistenden schließen lassen (z.B. Datenschutz-Dokumentationen, Gewährleistungsniveau, Kooperationsbereitschaft, Reaktionszeiten etc.)

10.3. Auftragsverarbeitung

Sollen Dienstleistende *Personenbezogene Daten* im *WHH*-Auftrag verarbeiten, bedarf es des Abschlusses eines Vertrags zur Auftrags*verarbeitung*. Hierin sind Datenschutz- und IT-Sicherheitsaspekte angemessen unter Berücksichtigung von Art. 27, 28 und Art. 32 DSGVO und ein angemessenes Gewährleistungsniveau zu regeln und deren Einhaltung angemessen zu überprüfen.

11. Rechte von Betroffenen Personen

11.1. Recht auf Auskunft

Betroffene Personen haben das Recht auf Auskunft über ihre von der *Welthungerhilfe* oder in deren Auftrag *verarbeiteten Personenbezogenen Daten*.

11.2. Auskunftserteilung

Bei der Bearbeitung von Auskunftsanträgen ist die Identität der Antragstellenden zweifelsfrei festzustellen. Bei begründeten Zweifeln an deren Identität können zusätzliche Angaben von den Antragstellenden angefordert werden. Kann die Identität nicht zweifelsfrei festgestellt werden, ist die Auskunft unter Angabe des Grundes schriftlich zu verweigern.

Die Auskunftserteilung (oder -verweigerung) erfolgt grundsätzlich schriftlich. Hat die *Betroffene Person* den Antrag auf Auskunft elektronisch gestellt, kann die Auskunft auch in Textform erteilt werden. Die Auskunft soll neben den *verarbeiteten Personenbezogenen Daten* der *Betroffenen Person*, auch die *Empfangenden Personen* von Daten, den Zweck der *Verarbeitung* sowie alle weiteren gesetzlich geforderten Informationen umfassen, damit die *Betroffene Person* die Rechtmäßigkeit der *Verarbeitung* selbst beurteilen kann. Der∗die *Datenschutzbeauftragte* berät über den erforderlichen Umfang der Informationspflicht. Auf besonderen Wunsch der *Betroffenen Person* werden die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt. Die zuständige IT-Abteilung legt den hierfür vorzusehenden Standard fest. Auf ausdrückliches Verlangen der *Betroffenen Person* ist eine Kopie der *Personenbezogenen Daten* der *Betroffenen Person* beizufügen.

11.3. Berichtigung

Betroffene Personen haben einen Anspruch auf Berichtigung ihrer *Personenbezogenen Daten*, wenn sich diese als unrichtig erweisen. Ebenso können sie die Vervollständigung unvollständiger *Personenbezogener Daten* verlangen. Berichtigungsanträgen ist unverzüglich nachzukommen.

11.4. Löschung

Betroffene Personen haben das Recht auf Löschung ihrer *Personenbezogenen Daten* unter den folgenden Voraussetzungen:

- die Kenntnis der Daten ist für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich;
- die *Betroffene Person* hat eine *Einwilligung* widerrufen und es fehlt an einer anderweitigen Rechtsgrundlage für die *Verarbeitung*;
- die *Betroffene Person* legt Widerspruch gegen die *Verarbeitung* zu Werbezwecken ein oder beruft sich auf ein Widerspruchsrecht aufgrund einer besonderen – zu begründenden – persönlichen Situation;
- es handelt sich um *Sensible Personenbezogene Daten*, deren Richtigkeit nicht bewiesen werden kann; oder

- es besteht eine anderweitige rechtliche Verpflichtung zur Datenlöschung.

Besteht eine Verpflichtung zur Löschung und wurden die *Personenbezogenen Daten* zuvor öffentlich gemacht, sind – soweit mit angemessenem Aufwand umsetzbar - weitere *Verantwortliche Personen* für die Daten*verarbeitung* über ein Löschbegehren der *Betroffenen Person* hinsichtlich aller Kopien ihrer *Personenbezogenen Daten* sowie aller Links zu diesen Daten zu informieren.

11.5. Einschränkung

Der *Betroffene Person* kann die *Einschränkung* der *Verarbeitung* ihrer *Personenbezogenen Daten* verlangen, wenn:

- die Richtigkeit der *Personenbezogenen Daten* strittig ist, jedoch nur so lange, wie die Richtigkeit durch die zuständige *Fachabteilung/Projekt* überprüft wird,
- die *Verarbeitung* unzulässig ist, die *Betroffene Person* die Datenlöschung aber ablehnt,
- die *Welthungerhilfe* die *Personenbezogenen Daten* für Zwecke der *Verarbeitung* nicht mehr benötigt, die *Betroffene Person* die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
- die *Betroffene Person* Widerspruch gegen die *Verarbeitung* aufgrund einer besonderen Situation eingelegt hat und die zuständige *Fachabteilung/Projekt* noch mit der Prüfung des Widerspruchs befasst ist.

11.6. Auskunftsfrist

Der *Betroffenen Person* ist spätestens innerhalb eines Monats nach Eingang des Antrags über die wesentlichen Maßnahmen, die auf den Antrag hin erfolgt sind, zu informieren.

11.7. Beschwerderecht

Jede *Betroffene Person* hat das Recht, sich über eine *Verarbeitung* ihrer *Personenbezogenen Daten* zu beschweren, sollte sie sich hierdurch in ihren Rechten verletzt fühlen. Beschwerden können gegenüber der∗dem *Datenschutzbeauftragten* erhoben werden; die∗der *Datenschutzbeauftragte* ist unabhängig und weisungsfrei. Ebenso können Beschwerden bei einer Aufsichtsbehörde eingereicht werden.

11.8. Beratungsauftrag der∗des *Datenschutzbeauftragten*

Die∗der *Datenschutzbeauftragte* steht bei der Wahrung der Rechte der *Betroffenen Person* beratend zur Verfügung.

12. Auskunftsersuchen Dritter über Betroffene Personen

Sollten *Dritte* Informationen über *Betroffene Personen* fordern, so beispielsweise über Spender∗innen oder *WHH-Mitarbeitende* oder von der *Welthungerhilfe* unterstützte *Projektbeteiligte*, ist eine Weitergabe von Informationen nur zulässig, wenn und soweit kumulativ:

- die Auskunft ersuchenden *Dritten* ein berechtigtes Interesse hierfür darlegen können, und
- eine gesetzliche Norm zur Auskunft gegenüber den *Dritten* verpflichtet, und
- die Identität der *Dritten* zweifelsfrei feststeht.

Im Zweifel über die Rechtmäßigkeit des Auskunftsersuchens ist die∗der *Datenschutzbeauftragte* vor Auskunftserteilung zu Rate zu ziehen. Besteht hinreichender Grund zu der Annahme, dass die Weitergabe der *Personenbezogenen Daten* an die *Dritten* zu einer Beeinträchtigung wesentlicher Rechte oder zu einer wesentlichen Gefährdung der *Betroffene Person* führt, dürfen die Daten nur mit vorheriger Zustimmung des Vereinsvorstands bzw. der Geschäftsführung der Stiftung weitergegeben werden. Bei ihrer Entscheidung haben

Vereinsvorstand/die Geschäftsführung die∗den *Global Privacy Officer* und die∗den *Datenschutzbeauftragte∗n* zu Rate zu ziehen.

13. Gefährdung oder Verletzungen des Schutzes von *Personenbezogenen Daten* („*Datenpanne*“)

13.1. Information des Information Security Expert

Sollte eine verantwortliche *Fachabteilung*, ein *Projekt* oder das verantwortliche *Landesbüro* Schwachstellen ihres jeweiligen Informationssicherheitskonzepts identifizieren, informieren sie darüber unverzüglich die∗den Information Security Expert im *Head Office* und fügen dieser Information einen Vorschlag zur Ausbesserung der Schwachstelle bei. Die∗der Information Security Expert wird sich – soweit erforderlich – mit der zuständigen IT Abteilung und der∗dem zuständigen *Country Privacy Officer* ins Benehmen setzen, einen Verbesserungsplan vorschlagen und dessen Umsetzung beratend und kontrollierend begleiten.

13.2. Informationspflicht im Fall einer schwerwiegenden Datenpanne

Die verantwortliche *Fachabteilung* oder das verantwortliche *Projekt* oder *Landesbüro* informiert unverzüglich die∗den *Global Privacy Officer* und die∗den *Datenschutzbeauftragte∗n*:

- im Fall einer vermuteten schwerwiegenden Verletzung des Schutzes *Personenbezogener Daten*, insbesondere wenn *Dritte* unrechtmäßig Zugang zu *Personenbezogenen Daten* erlangt haben. Die Meldung muss alle relevanten Informationen zur Aufklärung des Sachverhalts umfassen, insbesondere die vermutete Art der Verletzung, die empfangende Stelle, die *Betroffenen Personen* sowie Art und Umfang der betroffenen Daten. Die∗der *Global Privacy Officer* involviert im Benehmen mit der∗dem *Datenschutzbeauftragten* das *Data Incident Response Team*;

sowie

- bei Anfragen von Ermittlungsbehörden, Aufsichtsbehörden oder Rechtsstreitigkeiten mit Bezug zu *Personenbezogenen Daten*; bei Rechtsstreitigkeiten ist auch die Abteilung Legal & Compliance einzubinden.

13.3. Information der Aufsichtsbehörde und von *Betroffenen Personen*

Die Erfüllung einer etwaigen Informationspflicht gegenüber der Aufsichtsbehörde erfolgt ausschließlich durch die∗den *Datenschutzbeauftragte∗n*. *Betroffene Personen* werden durch die verantwortliche *Fachabteilung*/das verantwortliche *Projekt* in enger Abstimmung mit der∗dem *Global Privacy Officer* und der∗dem *Datenschutzbeauftragten* informiert. In kritischen Situationen ist die Abteilung Communications rechtzeitig in die Abstimmung der Kommunikation einzubeziehen.

14. Schulung

Alle *WHH-Mitarbeitenden* sind zu den Themen Datenschutz und Informationssicherheit angemessen zu sensibilisieren. *WHH-Mitarbeitende*, die ständig oder regelmäßig Zugang zu *Personenbezogenen Daten* haben, solche Daten *verarbeiten* (z.B. *WHH-Mitarbeitende* der Personalabteilung, des Spenderservice, oder *Projekt*mitarbeitende, die Daten von *Projektbeteiligten* verarbeiten) oder Systeme zur *Verarbeitung* solcher Daten entwickeln oder betreuen, sind in zusätzlich in geeigneter Weise über die datenschutzrechtlichen Vorgaben zu schulen. Die∗der *Global Privacy Officer* entscheidet über Form und Turnus der entsprechenden Schulungen und setzt sich hierüber mit der∗dem *Datenschutzbeauftragten* ins Benehmen.

15. Audits

15.1. Regelmäßige Überprüfung des Datenschutzniveaus

Um ein angemessenes Datenschutzniveau zu gewährleisten, werden relevante Prozesse unter der Verantwortung der Internal Audit regelmäßig durch interne oder externe Stellen überprüft. Im Falle der Feststellung eines Verbesserungspotentials sind Abhilfemaßnahmen zu definieren und entsprechend eines aufzustellenden Maßnahmenplan umzusetzen.

15.2. Dokumentations- und Informationspflicht

Die bei der Prüfung gewonnenen Erkenntnisse sind in einem Prüfbericht zu dokumentieren. Der Prüfbericht ist der∗dem *Datenschutzbeauftragten* und der∗dem *Global Privacy Officer* zu übergeben. Fachverantwortliche für den geprüften Prozess sind über das Prüfungsergebnis angemessen zu informieren.

15.3. Umsetzung von Verbesserungsmaßnahmen

Die im Bericht empfohlenen Verbesserungsmaßnahmen sind angemessen umzusetzen. Hierfür ist die jeweilige *Fachabteilung* oder das *Projekt*, in deren Verantwortung die zu verbessernden Prozesse durchgeführt werden, zuständig. Sie berichten über den Fortschritt der Umsetzung der Verbesserungsmaßnahmen und deren Abschluss an die∗den zuständige∗n *Country Privacy Officer* bzw. die jeweilige *Landesdirektion*. Bei Bedarf können Follow-up-Audits durchgeführt werden, durch welche die wirksame Umsetzung der empfohlenen Verbesserungsmaßnahmen überprüft wird.

16. Interne Ermittlungen

16.1. Beachtung Datenschutzrecht

Maßnahmen zur Sachverhaltsaufklärung, zur Vermeidung oder Aufdeckung von Straftaten oder schweren Pflichtverletzungen im Arbeitsverhältnis sind unter genauer Beachtung der einschlägigen gesetzlichen Datenschutzvorschriften durchzuführen. Insbesondere muss die damit einhergehende Datenerhebung und -verwendung zum Erreichen des Ermittlungszwecks erforderlich, angemessen und mit Blick auf die schutzwürdigen Interessen der *Betroffenen Person* verhältnismäßig sein.

16.2. Informationspflicht gegenüber der Betroffenen Person

Die *Betroffene Person* ist so bald wie möglich und geboten über die zu ihrer Person durchgeführten Ermittlungsmaßnahmen zu informieren.

16.3. Einbeziehung der∗des Datenschutzbeauftragten und der Arbeitnehmervertretung

Bei internen Ermittlungen ist die∗der *Datenschutzbeauftragte* hinsichtlich der Auswahl und Ausgestaltung der beabsichtigten Maßnahmen vorab einzubeziehen, um deren Konformität mit geltendem Datenschutzrecht zu überprüfen. Ebenfalls ist die jeweils zuständige Mitarbeitendenvertretung angemessen zu informieren bzw. entsprechend den rechtlichen Vorgaben einzubeziehen.

17. Rechenschaftspflicht

Die Einhaltung der Vorgaben dieser Richtlinie muss jederzeit nachgewiesen werden können. Hierbei ist insbesondere auf die Nachvollziehbarkeit und Transparenz getroffener Maßnahmen zu achten, so beispielsweise über zugehörige Dokumentationen.

18. Aktualisierung der *Policy*

Diese *Policy* ist regelmäßig auf ihren Anpassungs- oder Ergänzungsbedarf aufgrund Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen

zu überprüfen. Änderungen an dieser *Policy* bedürfen der Zustimmung durch die*den *Global Privacy Officer*. Sie sind umgehend schriftlich zu dokumentieren. Die *WHH-Mitarbeitenden* sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.

19. Meldepflicht und Konsequenzen bei Verstößen

Wer einen begründeten Verdacht auf Verstöße gegen diese Policy hat bzw. von solchen Verstößen weiß, ist verpflichtet, diese unverzüglich über das Welthungerhilfe Hinweisgeber-Portal ((www.welthungerhilfe.org/complaints);) zu melden.

Das Hinweisgeber-Portal gewährleistet angemessene Vertraulichkeit und ermöglicht die Abgabe vollkommen anonymer Meldungen.

Vorgesetzte oder nationalen Meldestellen der Welthungerhilfe, die entsprechende Hinweise erhalten, müssen diese vertraulich behandeln und über das Hinweisgeber-Portal an die Compliance-Abteilung melden.

Niemand, der in redlicher Absicht Hinweise auf Verstöße gibt, muss Nachteile oder sonstige Konsequenzen befürchten, auch dann nicht, wenn sich der Hinweis später als unbegründet herausstellt. Es liegt nicht in der Verantwortung der Mitarbeitenden und Mitwirkenden bzw. der Hinweisgebenden, Untersuchungen anzustellen, Beweise zu liefern oder eine Verletzung gegen diese Policy festzustellen.

Bewusst falsche Anschuldigungen und die Nichtmeldung von Verstößen gegen diese Policy verletzen den Welthungerhilfe Verhaltenskodex und diese Policy.

Verstöße gegen diese Policy können disziplinarische Maßnahmen bis hin zur fristlosen Kündigung und/oder die Annullierung der Zusammenarbeit zur Folge haben. Welthungerhilfe behält sich vor, Straftaten unter Beachtung des jeweils geltenden Rechts zur Anzeige zu bringen. Nähere Informationen liefern die folgenden Dokumente:

- *Leitfaden für Meldungen von Verstößen gegen den Verhaltenskodex*
- *Für Deutschland: Betriebsvereinbarung Hinweisgebersystem*

Internet: www.welthungerhilfe.org/complaints

Mathias Mogge
Generalsekretär/
Vorstandsvorsitzender

Christian Monning
Finanzvorstand