WORLD HEALTH ORGANIZATION (WHO)

PERSONAL DATA PROTECTION POLICY

(Effective as of 15th April 2024)

World Health Organization

TABLE OF CONTENTS

INTRODUCTION

This WHO Data Protection Policy (the "**Policy**") sets out the rules and principles relating to the Processing by and within WHO of Personal Data of individuals.

In pursuit of its mandate, WHO is often required to process Personal Data. This may include the need to share (transferring or receiving) Personal Data with Third Parties in the day-to-day operations of WHO. Third Parties may include suppliers of goods and services, contractors, consultants, implementing partners, collaborators, Member States, donors and other stakeholders.

The collection, analysis, publication and dissemination of health-related data is a core part of WHO's mandate. The Constitutional functions of WHO are, among others, to "establish and maintain such administrative and technical services as may be required, including epidemiological and statistical services; to promote (…) research in the field of health; and to provide information (…) in the field of health" (Article 2 of the WHO Constitution).

WHO is cognizant of the fact that it holds and processes sensitive medical data and data of vulnerable or marginalized individuals and groups of individuals, including children, which require careful handling and particular attention.

This Policy also considers the regulatory evolution in the field of data protection, as well as the *Personal Data Protection and Privacy Principles* of the United Nations ("**UN**") Privacy Policy Group ("**PPG**") adopted in September 2018 and endorsed by the High-Level Committee of Management ("**HLCM**") in October 2018, and the *WHO Data Principles*[1].

This Policy should be read in conjunction with other policies and procedures of WHO, notably the *Policy on Use and Sharing of Data Collected in Member States by WHO Outside the Context of Public Health Emergencies*[2], the *Policy statement on Data Sharing by WHO in the Context of Public Health Emergencies*[3], *the Information Disclosure Policy*[4] and , WHO's information technology and information security policies, section XXII of the eManual, as well as the WHO Staff Regulations and Staff Rules and the WHO Code of Ethics.

[1] https://www.who.int/data/principles
[2] https://www.who.int/publishing/datapolicy/en/
[3] http://www.who.int/publishing/datapolicy/en/
[4] https://intranet.who.int/homes/cre/ethics/disclosure/

This Policy may be complemented by operational guidelines (standard operating procedures) or other policies that will provide guidance on its implementation, supervision and accountability.

This Policy may be revised over time and will be evaluated by the WHO Secretariat after an initial two-year period following its entry into force.

Capitalized terms used in this Policy have the meanings ascribed to them in the "Definitions" section below or in the Policy.

DEFINITIONS

For the purposes of this Policy, the following definitions apply:

Anonymized Data	Information which does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the Data Subject is not or no longer identifiable.
Automated Processing	Automated individual decision-making (i.e. making a decision solely by automated means without any human involvement), including profiling (i.e. automated processing of Personal Data to evaluate certain elements about a Data Subject).
Consent	Clear Consent means any freely given and informed indication of an agreement by the Data Subject to the Processing of his/her Personal Data. It may be given either by a written or oral statement or other clear affirmative action. Explicit Consent means a very clear and specific statement of consent, which must be in writing. This could include electronic formats (such as sending an email, uploading a scanned document carrying the signature of the Data Subject, or using an electronic signature).
Data Controller	**T**he person or entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. A Data Controller has primary responsibility for the protection of Personal Data.
Data Processor	A person or entity which Processes Personal Data on behalf of, or under instructions from, the Data Controller.
Data Protection and Privacy Officer or DPPO	The officer who oversees the implementation of this Policy and performs the other functions listed in paragraph 6.3 of this Policy. The function of DPPO shall be performed by a WHO staff member.
Data Subject	An individual whose Personal Data is subject to Processing.
Health Data	Personal Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her current or past health status. This includes Personal Data derived

	from the testing or examination of a human body part or bodily substance, including from genetic data and biological samples.
Personal Data	Any information relating to an individual who is or can be identified from that information. Personal Data includes biographical data (biodata) such as name, sex, civil status, date and place of birth, country of origin, country of residence, individual registration number, occupation, religion and ethnicity, biometric data such as a photograph, fingerprint, facial or iris image, as well as any expression of opinion about the individual, such as assessments of the status and/or specific needs. Personal Data also includes data that, when combined with other data, can indirectly identify an individual.
Personal Data Breach	A breach of data security leading to the accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transferred, stored or otherwise processed.
Policy	The present World Health Organization Personal Data Protection Policy.
Processing (of Personal Data)	Any operation, or set of operations, automated or not, which is performed on Personal Data, including but not limited to the collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, transfer (whether in computerized, oral or written form), dissemination or otherwise making available, correction, or destruction.
Sensitive Personal Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic or biometric data uniquely identifying a natural person, Health Data or Personal Data relating to a natural person's sex life or sexual orientation.
Third Party	Any natural or legal person other than the Data Subject or WHO. Examples of Third Parties include governments of WHO Member States, international governmental organizations (IGOs), non-governmental organizations (NGOs), UN system agencies, private sector entities and other non-State actors, and individuals.
Vital Interests	An interest which is essential for the life of the Data Subject or that of another natural person.
WHO	The World Health Organization

1. SCOPE

1.1. This Policy applies to all Personal Data of living individuals held by WHO, contained in any form and processed in any manner.

1.2. The Processing of other, non-personal data, including Anonymized Data, does not fall within the scope of this Policy.

1.3. This Policy applies regardless of whether Processing takes place within one WHO office, between different WHO offices, or whether Personal Data are transferred to Third Parties.

1.4. The respective roles and responsibilities of WHO must be defined prior to the Processing of Personal Data to ensure accountability under this Policy. In some cases, WHO will be a Data Controller. In other cases, the Data Controller will be a Third Party and WHO will be a Data Processor.

a. As a Data Controller, WHO may only engage with Data Processors that provide appropriate commitment and assurance of meeting the requirements of this Policy or equivalent Personal Data protection standards. (See paragraphs 7.1 to 7.3, below).

b. As a Data Processor, WHO will notify Data Controllers of its Data Protection requirements, which, concerning WHO workforce Personal Data, shall always remain subject to the terms and conditions of employment of a Data Subject with WHO. WHO will not knowingly process Personal Data received that were not collected in compliance with this Policy. WHO will process Personal Data on documented instructions from the Data Controller or, concerning WHO workforce Personal Data, as authorized by the Director-General or his delegate.

2 GENERAL PRINCIPLES

A. Fair and Legitimate Processing of Personal Data

2.1 Processing of Personal Data may only be carried out on a legitimate basis and in a fair and transparent manner. WHO will only process Personal Data based on one or more of the following legitimate bases:

(i) **Consent**: the Data Subject has given Clear Consent to the Processing of the Personal Data or, in the case of Sensitive Personal Data as defined under section 3 below, the Data Subject has given Explicit Consent to the Processing of the Personal Data.

Wherever possible and practical, Consent should be the preferred basis for Processing Personal Data. However, given the exceptional circumstances in which WHO regularly operates (e.g. disease outbreaks and emergencies with health consequences, natural and man-made disasters, public scrutiny, etc.), WHO may not always be in a position to rely on this preferred basis for Processing Personal Data.

(ii) **Performance of a Contract**: the Processing of Personal Data is necessary: (a) for a contract to which WHO and the Data Subject are parties; (b) for WHO to address non-compliance with the terms and conditions of employment or engagement of the Data Subject with WHO; or, (c) in order to take steps at the request of the Data Subject prior to entering into a contract;

(iii) **Legal Obligation**: the Processing of Personal Data is necessary for compliance with a legal obligation to which WHO is subject;

(iv) **Vital Interests**: the Processing of Personal Data is necessary in order to protect the Vital Interests of the Data Subject or of another person;

(v) **Public Interest/Task**: the Processing of Personal Data is necessary for the performance of a task carried out in the public interest or in the exercise of WHO's public health mandate;

(vii) **Legitimate Interest**: the Processing of Personal Data is necessary for the purposes of the legitimate interests[5] pursued by WHO or a Third Party, provided such interests are not overridden by the interests or fundamental rights and freedoms of the Data Subject.

B. Transparency and Information

2.2 Where Personal Data relating to a Data Subject are collected from the Data Subject, he/she will receive the following information at the time when the Personal Data are collected or as soon as possible thereafter:

(i) the Personal Data concerned;

(ii) the purpose and period for which the Personal Data will be processed and stored;

(iii) any category of recipients of the Personal Data (to the extent known at the time of collection);

(iv) where applicable, information that the Personal Data are subject to Automated Processing;

(v) the Data Subject's right to request a copy of his/her Personal Data for the purposes of verifying its accuracy and completeness and to exercise the rights set out in Article 5, below; and

(vi) who to contact at WHO regarding requests concerning a Data Subject's Personal Data (Data Controller, DPPO).

2.3 Where Personal Data are collected through web-based applications, the information referred to in paragraph 2.2 may be provided to the Data Subjects through the terms of use or the privacy policy relating to the concerned website.

2.4 Where Personal Data are not collected through web-based applications, the Data Controller may determine, following consultations with the Data Protection and Privacy Officer (DPPO), that the provision of the information referred to in paragraph 2.2 is not compulsory if such provision would

[5] Legitimate interest may include a reputational/accountability interest of WHO for which the processing of the WHO workforce Personal Data is necessary to protect or preserve the reputation of WHO and/or WHO's best interests, for accountability purposes, or when the WHO workforce Personal Data is already in the public domain.

prove unnecessary under the circumstances (for example, as it may reasonably be considered that the Data Subject is aware of the information), or would involve a disproportionate effort.

C. Purpose specification and limitation

2.5 The Processing of Personal Data shall be relevant and limited to what is necessary to fulfill the specified purpose for which the Personal Data are collected, which will be determined prior to the commencement of any Processing.

WHO may further process Personal Data for purposes other than those specified at the time of collection: i) if such Processing is compatible with the original purpose; ii) if the new purpose is covered by a legitimate basis according to paragraph 2.1 above; iii) for statistical, historical or scientific purposes; iv) in the case of WHO workforce Personal Data for the purpose of protecting or preserving the reputation of WHO, WHO's best interests, for accountability purposes, or when Personal Data is already in the public domain; or (v) for the purpose of the performance by WHO of investigations or the exercise or defence of legal or administrative claims, or vi) for the purpose of WHO's compliance with international human rights standards, governmental, non-governmental and/or United Nations inter-agency agreements/protocols, and/or donor funding requirements pertaining to allegations of serious misconduct, including, but not limited to, any form of sexual misconduct, physical assault, fraud or abuse of authority.

D. Proportionality (Data minimization)

2.6 The Processing of Personal Data will be:

(i) adequate (sufficient to properly fulfil the specified purpose);

(ii) relevant (it will have a rational link to that purpose); and

(iii) limited to what is required to fulfil the purpose (and not excessive for the purpose for which the Personal Data are collected).

E. Accuracy

2.7 Personal Data should be accurate and, where necessary, kept up to date to fulfil the specified purpose for which the Personal Data were collected. All reasonable steps should be taken to ensure that the Personal Data are updated, where necessary. When inaccurate Personal Data is identified, it should be corrected or deleted without undue delay.

F. Confidentiality

2.8 Personal Data will be processed in a manner that ensures appropriate confidentiality of the Personal Data. Personal Data will be classified in accordance with an assessment of its sensitivity, in accordance with section XXII.3 of the eManual.

G. Time limitation for Storage

2.9 WHO will not keep Personal Data for a longer period than necessary for the purposes for which the Personal Data are Processed.

H. Security

2.10 With regard to the nature and sensitivity of Personal Data, appropriate organizational, physical and technical security measures will be implemented for both electronic and paper data to protect the security and integrity of Personal Data, including against Personal Data Breach, and to ensure its continued availability for the purposes for which the Personal Data are Processed.

2.11 WHO is under an obligation to ensure an adequate level of data security. WHO is required to protect the integrity, confidentiality, and availability of Personal Data by means of adequate technical and organizational security measures. Data security measures will be routinely reviewed and updated, as necessary, to ensure an adequate level of data protection relative to the degree of sensitivity and risk exposure of the Personal Data.

I. Data Breaches

2.12 Although WHO strives to have the best available data security in relation to the risks of a data breach, no security measure (whether technical, physical or organizational) is 100% guaranteed to prevent a breach. It is, therefore, not only important to provide adequate security, but to also have a reliable method for detecting any security breaches and acting on them quickly.

2.13 In the event of a Personal Data Breach, the Department of Information Management and Technology (IMT) or the relevant office, department, unit or individual who detected the breach shall report it to the DPPO without undue delay. The following information should be provided to the DPPO:

- how the breach was discovered and when;
- the nature of the breach, the categories of Personal Data affected, and the estimated number of Data Subjects concerned;
- the possible consequences of the Personal Data Breach; and
- any measures taken or proposed to be taken to address the breach.

IMT should also be informed and kept closely involved at all stages and in all measures taken in relation to any Personal Data Breach. The Department of Communications (DCO) should also be informed of any Personal Data Breach as early as possible.

WHO will promptly take all appropriate measures that reasonably within its power to limit the effects of a Personal Data Breach.

2.14 If, based on consultations with the DPPO and other relevant office, department or unit, as necessary, it is determined that the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons, and if technically and legally feasible, and provided it does not require disproportionate efforts, WHO will communicate the Personal Data Breach to the Data Subjects, individually or by a public statement.

J. Accountability

2.15 WHO will take appropriate measures in order to be able to demonstrate its compliance with the principles set out in this section 2.

3 SENSITIVE PERSONAL DATA

3.1 Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic or biometric data uniquely identifying a natural person, Health Data or Personal Data relating to a natural person's sex life or sexual orientation is considered as Sensitive Personal Data, the Processing of which requires particular measures.

3.2 Sensitive Personal Data require an additional level of protection, but given the different types of data falling within its scope, as well as the exceptional circumstances in which WHO regularly operates (e.g. disease outbreaks and emergencies with health consequences, natural and man-made disasters, public scrutiny, etc.), adequate measures should be contemplated and determined on a case-by-case basis.

3.3 The following principles will, however, always be considered in determining adequate measures:

(i) Sensitive Personal Data will be processed only when absolutely necessary, subject to Article 4 below;

(ii) Specific technical, organizational security measures, including confidentiality measures, and appropriate safeguards must be considered when Processing Sensitive Personal Data;

(iii) Sensitive Personal Data should be kept separate from other types of Personal Data, wherever possible and practical, and access to such Data should be controlled and limited; and

(iv) Conditions for Processing Sensitive Personal Data must be implemented before Processing, and the DPPO must be notified in advance of such Processing.

3.4 In addition, a specific legitimate basis will always be given for Processing Sensitive Personal Data:

(i) **Explicit Consent**: Explicit Consent from the Data Subjects should, wherever practically possible, be the preferred basis for Processing Sensitive Personal Data; or

(ii) **Vital Interests**: the Processing of Personal Data is necessary in order to protect the Vital Interests of the Data Subject or of another person; or

(iii) **Public interest/task**: Processing is necessary for reasons of overriding public interest, in particular based on WHO's public health mandate; or

(iv) **Legal proceedings**: Processing is necessary for the performance by WHO of investigations, or for the establishment, exercise or defence of legal claims; or

(v) **Archive, Scientific and historical purposes**: Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

4 RESEARCH DATA

4.1 Where the direct purpose of the Processing of Personal Data is scientific research (Processing of "Research Data"), the general principles and requirements of this Policy will apply unless they are likely to render impossible or seriously impair the achievement of that research purpose. The Processing of Research Data will in any case be carried out on an adequate legal basis, such as the public health mandate of the WHO or its institutions or, as applicable, a legitimate basis enshrined in paragraph 2.1 of this Policy.

4.2 Any restriction on the applicability of the requirements under this Policy, based on the conditions mentioned in paragraph 4.1 above, will:

(i) be limited to the minimum necessary to achieve the research purpose;
(ii) duly consider the fundamental rights of Data Subjects;
(iii) be properly documented;
(iv) be supported by appropriate safeguards and controls to ensure the security and confidentiality of the Personal Data at all times, such as, for example, technical and organizational measures for data minimization, encryption, pseudonymization or anonymization.

4.3 In particular, and subject to internationally-recognized ethical standards for scientific research being strictly adhered to, Research Data may be:

(i) processed for a different purpose than the purpose for which they were originally collected provided such secondary research purpose of Processing is compatible with the primary purpose of Processing; and

(ii) stored for a longer period than the period necessary for the fulfilment of the purpose for which they were collected, to the extent there is a legitimate purpose for retaining the data and provided such retention is regularly reviewed.

As a general principle, scientific research will not be deemed to be incompatible with the primary purpose of Processing Research Data, unless there are clear indications to the contrary or it can be clearly demonstrated otherwise.

4.4 Where the Research Data exemption mentioned in paragraph 4.1 above is relied on, it should be evaluated, in light of the risks to the rights and freedoms of the Data Subjects, whether a "data protection impact assessment" will be carried out. A data protection impact assessment is likely to be required if the Processing is not based on the informed consent of the Data Subjects as the legal basis and if such Processing is likely to imply substantive risks for the rights and freedoms of the Data Subjects. The safeguards implemented for the protection of the Research Data and the privacy of Data Subjects must be specifically reviewed, and the rights of Data Subjects must be balanced against the principle of freedom of research. Appropriate records of the Research Data that have been Processed, and information regarding the safeguards established, will be kept on file.

4.5 Where Personal Data are Processed for the purpose of scientific research, the rights of Data Subjects will be honoured, and may be limited only insofar as the exercise thereof is likely to make the achievement of the objectives of the research impossible or impedes it to a significant extent.

4.6 Regarding the transparency of Processing activities, adequate information will be provided to the Data Subjects, unless providing such information would be impossible or would involve

disproportionate efforts. In cases where Data Subjects are not informed directly, appropriate alternative measures must be taken, such as, for example, making the information regarding the Processing activities publicly available.

4.7 In case the exact purpose of the Processing of Research Data is not known at the time of data collection or transfer, the research purpose will be defined and documented adequately and in a timely manner, and any subsequent change to the purpose of Processing will be documented, as applicable.

4.8 For the avoidance of doubt, all other obligations related to Research Data, including, but not limited to, applicable regulatory requirements, and internationally-recognized professional and ethical standards and the WHO Research Ethics Review Committee's Guidelines, will be complied with.

5 RIGHTS OF THE DATA SUBJECTS

Data Subjects have the rights set out in this Article 5. The exercise of these rights and the processing of requests by Data Subjects will be done in accordance with paragraphs 6.4 and 6.5 below.

A. Information

The Data Subject has the right to receive the information mentioned in para. 2.2 where Personal Data relating to him/her are collected by WHO.

B. Access

The Data Subject has the right to request a copy of his/her Personal Data for the purposes of verifying its accuracy and completeness.

C. Rectification

The Data Subject has the right to request rectification of his/her Personal Data if it is inaccurate or incomplete. WHO may request the Data Subject to demonstrate the alleged inaccuracy or incompleteness. WHO will consider such requests and take appropriate action if it finds that the Personal Data is inaccurate or incomplete, subject to paragraphs 6.4 and 6.5 below.

D. Deletion

The Data Subject has the right to request deletion of his/her Personal Data. WHO will consider such requests and, subject to paragraphs 6.4 and 6.5 below, will take appropriate action if:

(i) such Personal Data are no longer necessary for the purpose of the Processing;

(ii) the Data Subject has withdrawn his/her consent to the Processing of the Personal Data which is based exclusively on such consent; or

(iii) the Personal Data must be deleted in order to comply with a legal obligation incumbent on WHO.

E. Restriction of the Processing of Personal Data

The Data Subject has the right to request that WHO restricts the Processing of his/her Personal Data.

F. Withdrawing Consent

The Data Subject has the right to withdraw his/her Consent at any time where WHO relied on his/her Consent to process his/her Personal Data. The withdrawal of consent will not affect any Processing of that Personal Data before its withdrawal.

G. Objection

The Data Subject has the right to object to the Processing of his/her Personal Data. If the objection is justified, WHO will no longer process the Personal Data concerned for the purpose(s) related to the objection. WHO will inform the Data Subject of the consequences of his/her objection, such as, for example, WHO being entitled to terminate any relevant contract or other relationship without incurring any liability. A request will not be considered justified if there are compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject or for the performance by WHO of investigations or for the establishment, exercise or defence of legal claims or to protect or preserve the reputation and/or interests of WHO.

H. Automated Processing

The Data Subject has the right not to be subject to Automated Processing, which may adversely affect the Data Subject's legal rights or similarly significantly affect him/her, unless it is necessary for entering into, or performance of, a contract between the Data Subject and WHO or is based on the Data Subject's Explicit Consent.

6 DATA PROTECTION AND PRIVACY OFFICER (DPPO)

A. Role and Responsibilities

6.1 With a view to overseeing the implementation of this Policy, the DPPO will be designated by the WHO Director-General and will be a member of the WHO Data Governance Committee (DGC). The DPPO will consult the Chief Information Officer (CIO) and the Office of the Legal Counsel (LEG), as appropriate.

6.2 The DPPO will be an independent function and report directly to the Director-General. Such reporting line will not affect, in any manner, his/her independence in the performance of his/her duties.

6.3 The DPPO's main functions and responsibilities will be exercised with objectivity and confidentiality, in consultation with the CIO and LEG, as appropriate, and are as follows:

a. Acting as first and main point of contact concerning all Personal Data Protection matters;

b. Providing advice, support and training on data protection and on this Policy;

c. Monitoring and reporting on compliance with this Policy;

d. Providing Data Subjects with information about their rights and handling requests from Data Subjects, as per the process established below under section B below;

e. As appropriate, engaging in discussions with other international organizations to share common challenges and best practices across United Nations agencies on Personal Data protection;

f. Ensuring that this Policy is regularly reviewed in light of relevant developments and making related recommendations to the Director-General;

g. Taking appropriate action in the event of a Personal Data Breach in accordance with paragraphs 2.13 to 2.16 above.

B. Contacting the DPPO

6.4 As mentioned under Article 5 above, Data Subjects are granted certain rights with respect to their Personal Data. All requests from Data Subjects must:

a. be submitted by the Data Subject by contacting the DPPO at the following email: dataprotection@who.int or at the following address: World Health Organization, Data Protection and Privacy Officer, 20 Avenue Appia, 1211 Geneva 11, Switzerland.

b. include sufficient information and documentation to prove that the person making the request is the individual to whom the Personal Data relates.

c. indicate the specific area and/or activities in relation to which WHO is Processing the Data Subject's Personal Data (e.g. recruitment procedures, registration for WHO meetings, procurement, etc.), along with an indication of the date on which the Personal Data were collected and other relevant information.

6.5 WHO may, following consultations with the DPPO, reject a request, in whole or in part, where:

a. there are grounds for believing that the request is manifestly abusive, fraudulent or obstructive to the purpose of Processing;

b. complying with the request proves to be impossible, inappropriate, or would involve a disproportionate effort;

c. the Processing of the Personal Data is necessary for archiving or statistical purposes, or to protect the interests of the Data Subject;

d. the Processing of the Personal Data is necessary for the performance of a task carried out in the exercise of official authority vested in the Organization;

e. the Processing of the WHO workforce Personal Data is necessary to protect and/or preserve the reputation of WHO, WHO's best interests, for accountability purposes, or when the WHO workforce Personal Data is already in the public domain;

f. the Processing of the Personal Data is necessary for the compliance with a legal obligation, the performance by WHO of investigations or the exercise or defence of legal claims;

g. the Processing of the Personal Data is necessary for the compliance with international human rights standards, governmental, non-governmental and/or United Nations inter-agency

agreements/protocols, and/or donor funding requirements pertaining to the investigation of allegations of serious misconduct, including, but not limited to, any form of sexual misconduct, abusive conduct, fraud or abuse of authority.

7 TRANSFER OF PERSONAL DATA TO THIRD PARTIES

A. Transfer to Contractors, UN system Agencies, Implementing Partners, etc.

7.1 Personal Data may be transferred or disclosed to Third Parties, including but not limited to contractors, vendors of goods and services (including cloud service providers), other UN system agencies, implementing partners and collaborating institutions, where the Third Party provides adequate safeguards to protect the Personal Data and the privacy rights of Data Subjects and following the conclusion of a written agreement or in accordance with a UN Protocol. Any transfer of Personal Data must be consistent with this Policy.

7.2 A Personal Data transfer agreement mentioned at paragraph 7.1, above, shall, at a minimum, include an undertaking on the part of the Third Party that:

a. an adequate level of protection (i.e. sufficient taking into account the type of Personal Data concerned, and the purpose of the disclosure) will be provided as regards to the Personal Data transferred by WHO;

b. the supplied Personal Data will be used only in accordance with the terms of the agreement, and not for any purpose not contemplated in the agreement;

c. all Personal Data will be returned to WHO and/or destroyed at any time upon request by WHO and, unless otherwise agreed, at the expiration or termination of the agreement. The Third Party shall confirm to WHO in writing that it has complied with the foregoing no later than seven (7) days after receipt of the notification from WHO;

d. sufficient security safeguards (such as encryption, storage in secure location, setting up of antivirus software and firewalls, etc.) will be implemented to prevent Personal Data Breach;

e. none of the work will be subcontracted without WHO's prior consent; and

f. WHO will be promptly notified in the event that a Personal Data Breach occurs and that the Third Party will cooperate with WHO in taking appropriate action in response to the Personal Data Breach, including appropriate measures to limit the effects of a Personal Data Breach.

7.3 Notwithstanding paragraphs 7.1 and 7.2, above, where WHO is the Data Processor, it may only engage with sub-processors with the consent of the Data Controller, and where the sub-processors agree to comply with the same obligations with regard to Personal Data Protection as agreed between WHO and the Data Controller.

7.4 It is recognized that it may not always be possible to conclude a written agreement prior to sharing Personal Data with certain partners and in certain exigent circumstances, such as disease outbreaks and emergencies with health consequences. In such circumstances, and where transfers are necessary to protect the Vital Interests of affected persons, all steps should be taken as soon as possible after the relevant outbreak or emergency, to protect the transferred Personal Data, including through pursuing a written agreement.

B. Disclosure to Authorities

7.5 Nothing in or relating to this Policy shall be deemed as regulating or limiting the communication by WHO of information – including Personal Data – to appropriate authorities to facilitate the proper administration of justice.

7.6 As such, this Policy shall not prejudice any cooperation that may take place between WHO and government entities and law enforcement agencies (such as police authorities or national courts).

C. No Commercial Disclosure

7.7 WHO will not sell Personal Data to Third Parties.

8 PRIVILEGES AND IMMUNITIES OF WHO

8.1 Nothing contained in or relating to this Policy, or done pursuant to it, shall be construed as a waiver of any of the privileges and immunities enjoyed by WHO under national or international law, and/or as submitting WHO to any national court jurisdiction. Without limiting the generality of the previous sentence, any disclosure of Personal Data in response to a request for disclosure in accordance with this Policy, will not constitute a waiver, express or implied, of any of the privileges and immunities of WHO.

9 ENTRY INTO FORCE; REVIEW AND AMENDMENT OF THIS POLICY

9.1 This Policy enters into force on the date it is signed by the WHO Director-General. It will be implemented progressively over a period of two years following its entry into force. Personal Data hosted by WHO should be fully compliant with the Policy. All new Information Technology systems introduced by WHO following its entry into force should be fully compliant with the Policy. Information Technology systems introduced by WHO before its entry into force might not be compliant with the Policy due to technical limitations.

9.2 This Policy will be evaluated by the WHO Secretariat after the initial two-year transition period and will be reviewed by the Secretariat thereafter from time to time. WHO may amend this Policy at any time, without prior notification, by posting the new version on its website at www.who.int.

9.3 Any amendments to this Policy shall become effective on the date the revised Policy is posted on WHO's website. Personal Data will be handled in accordance with the Policy that was in effect at the time of collection.