International Agency for Research on Cancer



IARC Data Protection Policy

- .
- · ·

Table of Contents

I. UN Principles on Personal Data Protection and Privacy	2
I.1. Purpose	2
I.2. Principles	3
II. General aspects of Data Protection and Privacy at IARC	4
Introduction	4
II.1. Principles of Scientific Data Processing	4
II.2. Sensitive Data	4
II.3. Research Data Processing	5
II.4. Rights of the Data Subjects	6
II.5. Data Retention / Storage	6
II.6. Transfer of personal data internally and to / from third parties	7
II.7. Security	7
II.8. Data breaches	7
II.9. Accountability	8
II.10 Privileges and Immunities of IARC/WHO	8

I. UN Principles on Personal Data Protection and Privacy

The Personal Data Protection and Privacy Principles for UN System Organizations, UN-HLCM 2018 (the "Principles"), adopted by the UN High-Level Committee on Management at its 36th Meeting on 11 October 2018, are available under:

https://unsceb.org/personal-data-protection-and-privacy-principles

I.1. Purpose

10 The Principles set out a basic framework for the processing of "personal data", which is defined as information relating to an identified or identifiable natural person ("data subject"), by, or on behalf of, the United Nations System Organizations in carrying out their mandated activities.

20 These Principles aim to:

(i) harmonize standards for the protection of personal data across the United Nations System Organizations;

(ii) facilitate the accountable processing of personal data for the purposes of implementing the mandates of the United Nations System Organizations; and

(iii) ensure respect for the human rights and fundamental freedoms of individuals, in particular the right to privacy.

30 **Scope:** These Principles apply to personal data, contained in any form, and processed in any manner.

40 The United Nations System Organizations are encouraged to adhere to these Principles and may issue detailed operational policies and guidelines on the processing of personal data in line with these Principles and each Organization's mandate.

50 Personal data should be processed in a non-discriminatory, gender sensitive manner.

60 Where appropriate, these Principles may also be used as a benchmark for the processing of nonpersonal data, in a sensitive context that may put certain individuals or groups of individuals at risk of harms.

70 United Nations System Organizations should exercise caution when processing any data pertaining to vulnerable or marginalized individuals and groups of individuals, including children.

80 In adherence with these Principles, the United Nations System Organizations should conduct riskbenefit assessments or equivalent assessments throughout the personal data processing cycle. Implementation of these Principles is without prejudice to the privileges and immunities of the relevant United Nations System Organizations concerned.

I.2. Principles

10 Fair and legitimate processing

The United Nations System Organizations should process personal data in a fair manner, in accordance with their mandates and governing instruments and on the basis of any of the following: (i) the consent of the data subject; (ii) the best interests of the data subject, consistent with the mandates of the United Nations System Organization concerned; (iii) the mandates and governing instruments of the United Nations System Organization concerned; or (iv) any other legal basis specifically identified by the United Nations System Organization concerned.

20 Purpose specification

Personal data should be processed for specified purposes, which are consistent with the mandates of the United Nations System Organization concerned and take into account the balancing of relevant rights, freedoms and interests. Personal data should not be processed in ways that are incompatible with such purposes.

30 Proportionality and necessity

The processing of personal data should be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal data processing.

40 Retention

Personal data should only be retained for the time that is necessary for the specified purposes.

50 Accuracy

Personal data should be accurate and, where necessary, up to date to fulfil the specified purposes.

60 Confidentiality

Personal data should be processed with due regard to confidentiality.

70 Security

Appropriate organizational, administrative, physical and technical safeguards and procedures should be implemented to protect the security of personal data, including against or from unauthorized or accidental access, damage, loss or other risks presented by data processing.

80 Transparency

Processing of personal data should be carried out with transparency to the data subjects, as appropriate and whenever possible. This should include, for example, provision of information about the processing of their personal data as well as information on how to request access, verification, rectification, and/or deletion of that personal data, insofar as the specified purpose for which personal data is processed is not frustrated.

90 Transfers

In carrying out its mandated activities, a United Nations System Organization may transfer personal data to a third party, provided that, under the circumstances, the United Nations System Organization satisfies itself that the third party affords appropriate protection for the personal data.

100 Accountability

United Nations System Organizations should have adequate policies and mechanisms in place to adhere to these Principles.

II. General aspects of Data Protection and Privacy at IARC

Introduction

This IARC Data Protection Policy (the "Policy") addresses the processing of personal data for scientific purposes by IARC personnel, as well as third parties collaborating with or acting on behalf of IARC. The Policy builds on the UN Principles as well as the WHO regulatory framework, and translates the principles enshrined in these documents to the specific framework at IARC. The Policy does not address the internal IARC data processing for administrative purposes (covered separately).

II.1. Principles of Scientific Data Processing

10 Personal data shall be processed in accordance with the UN Principles, the WHO regulatory framework and this Policy. The UN Principles shall form an integral part of this Policy. IARC is committed to strive for the highest level of protection as it processes personal data, and will always respect the rights and freedoms of data subjects.

20 Personal data shall be processed for specified and lawful research purposes, and in a manner that is proportional to these purposes. IARC is an international research body, and is tasked with the execution and coordination of research in the field of public health and more specifically, research on cancer. In order to achieve its general interest mission and public health mandate –hereinafter referred to as IARC's "public task", IARC must have access to, and be able to process personal data.

30 IARC shall ensure that such processing is carried out on a valid legal basis, such as, inter alia, the public task of IARC, the consent of a data subject, or if the processing serves a vital interest of a data subject or a third party. As part of its mandate, IARC shall also protect the freedom of research and the fundamental rights of researchers to conduct such research. To the extent required, IARC shall balance these fundamental rights and shall aim to achieve a concordance between those fundamental rights in case of a conflict. Any research conducted at IARC will in any case always be subject to review and approval by the IARC Ethics Committee.

40 IARC shall ensure that the personal data is accurate, and that the processing is limited to the minimum required to achieve the public task of the organization. IARC shall also ensure that data protection is embedded into the design of its procedures and the technical setup of the organization. In addition, IARC shall maintain a training and awareness programme for IARC personnel, and shall ensure that third parties collaborating with, or acting on behalf of IARC are made aware of the data protection requirements of the organization.

II.2. Sensitive Data

10 As part of its public task, IARC may process special categories of data ("sensitive data"), in particular health data to the extent such processing is necessary and proportionate.

20 IARC may also process other special categories of data, such as data revealing political or philosophical/ethical or religious beliefs, trade union membership, sex life or sexual orientation to the extent such data processing is absolutely necessary for the achievement of IARC's processing activities in the field of cancer research.

30 Health data shall be processed when necessary for the achievement of IARC's public task and mandate, or based on the data subjects' explicit consent.

II.3. Research Data Processing

10 IARC shall act as a data controller of research data, and shall encourage its partners and collaborators to ensure full compliance with applicable data protection legislation and the highest standards of data protection.

20 In case of the processing of personal data for research purposes, IARC shall ensure an adequate level of transparency that is proportionate to the risks to the rights and freedoms of data subjects. IARC shall also, at minimum, adhere to the principles and procedures as laid out in the WHO regulatory framework that are applicable to the processing of personal data for research purposes.

30 It shall be IARC's aim and priority to process research data in a way that minimizes the risk of an identification or re-identification of data subjects. Researchers at IARC shall always carefully assess and document whether the research purposes can be achieved with fully anonymous or at least pseudonymous/de-identified data.

40 In case the information or re-consenting of data subjects would require a disproportionate effort or is not achievable for IARC due to technical or methodological limitations, IARC shall provide relevant information publicly accessible and shall assess the compliance of such processing, e.g., by consulting the IARC Ethics Committee and/or the IARC Data Protection Officer (the "IARC DPO"). These exemptions shall only apply to the extent the processing is carried out for scientific purposes.

50 IARC will often conduct secondary use of personal data, as data is mostly collected by collaborators and/or national bodies. In case of a secondary use, IARC shall assess the legality of the initial data processing, and shall ensure that data is legally transferred to IARC. IARC must also ensure that the purpose of the processing is compatible with the original data processing purpose, and that the secondary use does not affect data subjects inadequately. Notably, as IARC conducts non-commercial research in cancer, such processing for research purposes shall not be considered to be incompatible with the primary processing purpose unless specific restrictions follow from the consent procedure of the primary data collection, or if regulatory restrictions apply in relation to the primary data controller. IARC shall aim to obtain personal data for secondary research purposes on a controller-to-controller basis.

60 IARC hosts a research biobank with biological material derived from human subjects. Such samples do not per se constitute personal data. To the extent such samples are accompanied by personal data, this Policy applies to accompanying data. In case data is derived from samples, either by IARC or a third party, and such data qualifies as personal data, this Policy shall also apply to data derived from samples. In case IARC transfers samples to a third party, and it is the intention of the third party to derive data from the samples that would qualify as personal data, IARC shall ensure that the principles and procedures for the transfer of personal data, as stipulated in this Policy, will apply.

II.4. Rights of the Data Subjects

10 IARC shall respect the rights of data subjects and shall provide information in a concise, transparent, intelligible and easily accessible form, using clear and plain language. It shall be noted that IARC is rarely the institution collecting the data, as IARC is often conducting research that is based on the secondary use of personal data, or the data collection may be implemented by local collaborator that acts as the initial data controller. In this case, IARC shall assess whether the initial data controller has provided the data subjects with adequate and appropriate information on the processing of personal data; and IARC shall provide additional information regarding the processing at IARC, either directly to the data subjects or, if that is not feasible or requires disproportionate efforts, via publicly accessible information that is aligned with the requirements stipulated by applicable data protection legislation and/or principles. Such additional information shall also provide information on the processing of data from data collections that date back to the times before modern data protection regulations were put in place ("legacy collections").

20 Information to be provided must include the controller's identity ("IARC") and contact information, the intended purposes of the processing activities, and, where applicable, that the data will be transferred to another entity or to a third country. Additionally, IARC must provide notice of the data subjects' rights to access, rectification, erasure and to object to processing, as well as notice of the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

30 IARC must adhere to these rights and must set up effective processes for the handling of data subject requests. Such requests shall be addressed within 30 days from the date of submission, unless exceptional circumstances require a longer period.

40 The rights of data subjects may need to be balanced against the freedom of research, and in case IARC is not able to adhere to a data subject's requests in order to protect the quality of cancer research, or if such adherence is technically not feasible, this shall be properly documented and communicated to the data subject. Any such limitation of the rights of data subjects shall comply with the principles enshrined in the WHO regulatory framework.

II.5. Data Retention / Storage

10 As a default, IARC shall keep data only as long as the data is needed to serve the research purposes of the organization, and as long as IARC has a legal basis to process such data. Relevant information shall be provided to the data subjects, e.g., via information sheets or publicly accessible information.

20 Due to the nature of the research being conducted at IARC, personal data may be retained for an extensive period, in some cases even for an indefinite period of time. This is depending on the requirements of the research, e.g., in cases where IARC needs to follow cancer development and/or mortality over a long time span.

30 IARC shall periodically, at least once per calendar year, review the retention of personal data for research purposes, and shall also review whether such data must be kept in a person-identifiable manner or whether data could be anonymized, further pseudonymized or aggregated.

II.6. Transfer of personal data internally and to / from third parties

10 The transfer of personal data within IARC shall not be restricted as IARC serves as the data controller to the data, and as the different research groups within IARC all serve non-commercial cancer research purposes. In case of an internal transfer of data, or if data is made accessible internally to another research group, IARC shall ensure that the internal recipient will act on a legal basis in compliance with this Policy, and that all data processing restrictions are also adhered to by the internal recipient of data.

20 IARC may transfer personal data to a recipient outside of IARC, provided the recipient offers appropriate safeguards, only if at least one of the following conditions is met:

(a) the recipient is established in a country or international organization which ensures an adequate level of data protection; or

(b) the data subject has consented to such transfer; or

(c) the transfer is needed for the conclusion or performance of a contract, for important reasons of public interest, or to protect the vital interests of a data subject or a third person.

30 The transfer will always be based on a specific Data Transfer Agreement (DTA). The Data Transfer Agreement will specify the legal basis for the transfer and will ensure that the data recipient will adhere to data protection standards that are at least compliant with the standards enshrined in this Policy.

40 As a general principle, IARC shall always assess, prior to any transfer, whether the recipient can also achieve its scientific purposes by processing the data remotely on the IARC Scientific IT Platform. If so, IARC shall recommend the recipient to process such data on the IARC infrastructure in order to avoid a physical transfer of data, thereby maximizing its safeguards and data protection measures.

50 In case IARC makes personal data accessible to a third party ("recipient") remotely on the IARC Scientific IT Platform, IARC shall ensure that such third party adheres to IARC's standards of data protection and data security. Such access will be governed by a specific Data Use Agreement (DUA) that outlines the specific purpose for which the recipient is allowed to process the data.

II.7. Security

10 IARC shall ensure the confidentiality, integrity, availability of personal data by implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risks for the rights and freedoms of data subjects. The IARC security program shall be aligned with state of the art security frameworks, e.g. ISO 27001 and ISO 27701. IARC shall ensure that any collaborator working with IARC, and in particular, those receiving personal data from IARC, shall have a security program in place that is at least following the IARC standards.

II.8. Data breaches

10 For the purpose of this Policy, a data breach is defined as an unauthorized acquisition, access, or use of personal data that compromises the security, integrity or confidentiality of such data.

20 IARC shall notify data subjects, whose personal data has been, or is reasonably believed to have been accessed, acquired, or disclosed as a result of a breach, if the breach poses a risk of significant harm

as defined by the IARC data breach policy. In case that IARC had received such data from a third party, IARC shall immediately inform the third party and shall offer assistance to such third party in addressing the breach. In case IARC has transferred data to a third party, and a data breach occurs at the third party, IARC shall take appropriate measures to address such breach and to notify data subjects if the breach at the third party poses a risk of significant harm.

30 The IARC Committee for Information Security Oversight oversees the implementation of IARC's Information Security Policy and ensures that the organization responds to new developments in relation to information security in a timely and informed manner. This also include, should such a case arise, addressing any major security concern with potential impact to the confidentiality, integrity or availability of data. To this effect, IARC has implemented a dedicated data breach policy and has rolled out relevant processes that set out internal procedures for the handling of data breaches.

II.9. Accountability

10 Data subjects may submit a complaint to IARC in case those data subjects are of the opinion that IARC, or a third party acting on behalf of IARC, has violated the data subjects' data protection rights. Data subjects may contact IARC by letter, or electronically by sending an electronic mail to the IARC Data Protection Officer: <u>dpo@iarc.fr</u>.

20 Any such complaint, or any data subject request, shall be reviewed by IARC without any undue delay. In case of a data subject request, IARC shall respond within 30 days from the submission of the request, in case of a complaint, IARC must decide on the complaint within two months of receipt. It may extend that time limit, if it considers the complaint to rest on complicated facts or legal considerations and gives prior notice to the complainant.

30 Any dispute, controversy or claim arising out of or relating to the processing of personal data under this Policy and brought by data subjects other than IARC staff, shall be resolved through the available alternative dispute resolution mechanisms. IARC may also refer such disputes to the legal redress mechanisms established by WHO in case such referral will foster the ability of the data subject to exercise her/his rights.

II.10 Privileges and Immunities of IARC/WHO

10 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 IARC/WHO under national or international law, and/or as submitting IARC/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 IARC/WHO.