Welcome the stranger.
Protect the refugee.

HIAS DATA PROTECTION POLICY

Effective: March 31, 2022

I. Policy Statement

In keeping with its vision, values and as referenced in our Code of Conduct Standards, all HIAS, Inc. ("HIAS") staff and associated personnel are responsible for the use of information, assets and resources to which they have access. At HIAS, the privacy and security of our clients, employees, donors, website and digital content users is of paramount importance. HIAS is committed to protecting the data shared with us. This Data Protection Policy explains how HIAS staff and associated personnel must control and process information used directly or indirectly to identify an individual. Such personal information, also known as Personally Identifiable Information, includes name, address, email address, date of birth, identification numbers, private and confidential information, sensitive information and medical and psychosocial history and bank details, regardless of format ("Personal Data"). Key data protection terms used in this Policy are defined in ***Annex 1***.

II. Purpose

HIAS is committed to compliance with data protection laws, including collecting, processing, storing and destroying all information in accordance with, as legally applicable, the: (a) Regulations (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, known as the General Data Protection Regulation ("GDPR"); (b) data protection laws of the countries in which HIAS operates; and (c) any other associated legal or regulatory body of rules or codes of conduct that apply to HIAS' business and/or the information HIAS processes and stores. This Policy defines HIAS' procedures for ensuring such compliance.

Where any provision of this Policy conflicts with a law or regulation, the law or regulation shall supersede the conflicting provision. This Policy replaces and supersedes the "HIAS Privacy Policy" (which took effect on March 14, 2021).

Headquarters 1300 Spring Street, Suite 500 • Silver Spring, MD 20910 • 301 844 7300 • hias.org
SILVER SPRING • NEW YORK • WASHINGTON DC • CARACAS • LESVOS • N'DJAMENA • NAIROBI • PANAMA CITY • QUITO • SAN JOSE • TEL AVIV • VIENNA

III. Applicability

This Policy binds all staff and personnel employed or engaged by HIAS, whether in the United States, in our country offices or in our resettlement support centers, including, permanent staff, fixed term and temporary staff, third-party representatives or sub-contractors, volunteers, interns and agents. For purposes of this Policy, the foregoing parties are collectively referred to as "HIAS Staff and associated personnel." Adherence to this Policy is mandatory and non-compliance may lead to disciplinary action.

IV. Types of Data Covered by this Policy and Purposes for Data Processing

HIAS collects, stores and processes information relating to clients/beneficiaries, employees, private donors and users of its website and digital content or communications. This type of information consists of the following:

A. Employee Records

The HIAS Human Resources Department ("HIAS HR") is responsible for collecting and processing the information of all new employees at the time they join HIAS and in accordance with HIAS' HR policies. HIAS HR uses this information for our administrative, HR and payroll functions.

B. Client/Beneficiary Records

As a global refugee agency, HIAS maintains clients' records. These records consist of case files containing biographic and demographic data, intake notes and, at times, sensitive health information. As an organization receiving funding from various sources (including, but not limited to, national, international, private donors and U.S. federal government funding), HIAS maintains records in compliance with funder requirements and uses this information to render effective services to the clients HIAS serves. At all times, HIAS must maintain such records in compliance with applicable data protection and privacy laws of the countries in which HIAS operates and with relevant international standards. To the extent there are conflicting applicable standards, the higher standards shall apply.

C. Information about Private Donors

HIAS collects information about its private donors and amounts raised by donors. When a private donor wishes to donate through HIAS' website, the donor must register its information there. A donor will provide information such as name, company name, email, address, home or work address, phone number, credit-card number, and other relevant data. This information is used by HIAS to identify the donor, provide the donor with mailings and communications, and process the donor's billing information.

D. Visitors and Users of HIAS' Website and Digital Content or Communications

HIAS collects Personal Data from users in association with donations, user registration, newsletters and other activities, when relevant. HIAS collects and processes Personal Data provided by users into our website's forms, such as when users register for events or sign up for information and newsletters. HIAS also uses Personal Data in communication with registered users, such as for sending the HIAS newsletter or soliciting funds. HIAS sends targeted social media posts to users based on user analytics and uses information about donations, actions taken or users' content preferences to generate custom email solicitations for donations. Information about computer hardware and software is automatically collected by HIAS, including IP address, browser type, domain names, access times and referring website addresses, for the operation of HIAS' services, to maintain the quality of the HIAS website and to provide general statistics regarding use of the HIAS website.

V. HIAS' Role and Responsibilities as Data Controller or Data Processor

The respective roles and responsibilities (as a controller or a processor) of HIAS must be defined prior to the collection and further processing of Personal Data to ensure accountability under this Policy.

As a controller, HIAS may only engage with processors that provide appropriate commitment and assurance of meeting the requirements of this Policy and applicable privacy laws. As a joint controller, HIAS shall agree in writing with other controllers as to the responsibilities of each and shall disclose the arrangement to the data subject where appropriate.

As a processor, HIAS will notify data controllers of its data protection requirements and will not knowingly process Personal Data it receives that was not collected in compliance with this Policy or applicable data protection laws. HIAS may only process data on documented instructions from the controller, subject to any pre-existing obligations that HIAS has disclosed to the controller. HIAS may only engage with sub-processors upon consent of the controller and where the sub-processor agrees to assume the same data protection obligations as HIAS made to the controller.

VI. Data Protection Principles

When HIAS staff and associated personnel control and process information that is used, directly or indirectly, to identify an individual, they do so using the following data protection principles:

A. Legitimate and Fair Processing

a. One or more legitimate bases is required for the processing of Personal Data.
b. The legitimate bases are:
    i. the consent of the data subject, or their lawful representative
    ii. where appropriate ("consent");
    iii. to prepare for or perform a contract with the data subject, including a contract of employment ("contract");
    iv. to protect the life, physical or mental integrity of the data subject or another person ("vital interests");
    v. to protect or advance the interests of people HIAS serves, and particularly those whose interests HIAS is mandated to protect or advance ("HIAS' legitimate interest" as well as the "beneficiary interest");
    vi. compliance with a public legal obligation to which HIAS is subject ("legal obligation"); or
    vii. other legitimate interests of HIAS consistent with its mandate, including the establishment, exercise or defense of legal claims, or for HIAS accountability ("other legitimate interests").
c. Consent, often supported by other legitimate bases, is the preferred basis for processing. In some cases, obtaining consent may be impractical, including

because: the data subject is an under-13 child or is a child whose age cannot be determined, and consent cannot be sought from a child's representative; the capacity of the data subject to consent cannot be reasonably assessed and substitute, alternative consent is unavailable; or there is urgency and the timely grant of consent by the data subject is not expected.

d. Personal Data shall be processed in a manner that is transparent to the data subject and in conformity with this Policy.

B. **Purpose Specification**

a. Personal Data shall be processed for specified and limited purposes which are consistent with the mandate of HIAS and are determined prior to the time of
    i. collection.
b. HIAS may further process Personal Data for purposes other than those specified at the time of collection:
    i. if consent is obtained for further processing;
    ii. if such further processing is compatible with the original purposes and the risks of further processing do not outweigh the benefits it entails for the data subject;
    iii. if HIAS is required to process further for statistical, historical or scientific purposes;
    iv. to establish HIAS accountability; or
    v. for the establishment, exercise or defense of legal claims.

C. **Necessity and Proportionality**

a. The processing of Personal Data shall be relevant, limited and adequate to what is necessary in relation to the purpose(s) specified for processing.
b. This principle requires, in particular, ensuring that the Personal Data collected are not excessive for the purposes for which they are collected, and that the period for which the data are stored in the HIAS information asset is no longer than necessary, in conformity with the data retention requirements of this Policy.

D. **Accuracy**

a. Reasonable efforts shall be made to process Personal Data with accuracy and, to the extent possible, in order to fulfill the specified purposes of processing, the Personal Data shall be kept accurate and up-to-date.
b. The accuracy of the Personal Data to be retained shall be reassessed periodically, according to the following principles:
    i. frequency of an accuracy review will depend on factors such as the relative time sensitivity of the Personal Data;
    ii. determination of reassessment frequency shall be substantiated and documented; and
    iii. Personal Data in archives need not be reassessed, corrected or kept current.

E. **<u>Security</u>**

a. Personal Data shall be classified in accordance with a contextual assessment of its sensitivity, in accordance with HIAS information security standards.
b. Appropriate organizational, administrative, physical and technical safeguards and procedures shall be implemented to protect the security of Personal Data, including from accidental or unauthorized destruction, loss, alteration, disclosure, access, or unplanned loss of availability. Such measures may include log-in access, and changes to or deletion of Personal Data.

F. **<u>Limited Retention</u>**

a. Personal Data shall be retained in the HIAS information assets as follows:
    i. Permanently, if and only if the criteria under HIAS' policies and procedures on archiving are met; and
    ii. For the time required to achieve the purposes for which the Personal Data were collected.
b. Those responsible for stipulating and implementing appropriate retention schedules shall substantiate and document:
    i. how long the Personal Data is needed for the intended purpose(s);
    ii. after which period of time the data will become stale or no longer useful for the intended purpose(s);
    iii. the appropriate retention period for the Personal Data based on assessment of retention needs; and

iv. how to safely and appropriately destroy or archive the Personal Data at the end of the determined retention period.
    1. Note: Retention periods exceeding 10 years require additional substantiation.

G. **Notice of Personal Data Processing**

a. HIAS shall provide to the data subject transparent, appropriate and timely information when collecting their Personal Data.
b. When Personal Data are collected by HIAS (as controller) from a source other than the data subject, HIAS is obligated to make reasonable efforts to respond to data subjects' requests regarding Personal Data held by HIAS information assets.

H. **Data Subject Requests to Interact with their Personal Data**

a. Access, correction, deletion, objection and restriction to processing of Personal Data, portability of their Personal Data and objection to automated decision-making may be requested, subject to the conditions below, by an individual who provides sufficient evidence of being the relevant data subject or data subject's lawful representative:
    i. such requests shall be limited to Personal Data within HIAS' information assets that directly identify the data subject and not to data that could indirectly identify the data subject; and
    ii. where such requests relate to Personal Data held in unstructured format, including written reports, and other files from which Personal Data extraction is not reasonably available, HIAS would generally decline to fulfill the request, unless overriding considerations demand otherwise. Such overriding considerations could include upholding the fundamental rights and freedoms of individuals.
b. Data subject requests shall be addressed by HIAS in accordance with the mechanism set out in HIAS data subject request procedure, taking into account possible overriding considerations in the application of this Policy and the provisions below.

I. **Access**

a. Unless it adversely affects the rights and freedoms of others, upon request, the data subjects or lawful representatives shall be provided with confirmation as to

whether Personal Data concerning the data subject are being processed and, where that is the case, information about requested categories of Personal Data held by HIAS.

b. Access to HIAS archives shall be provided in accordance with applicable policies and procedures specific to archives.

J. Correction

a. A request from the data subject or lawful representative to update or correct Personal Data should be granted, unless the requested change would be inaccurate, or the data are contained in a record held in the HIAS archives.
    i. In order to preserve the integrity of HIAS archives, a note may be included in the relevant archival file to indicate that a correction request has been made.

K. Deletion

a. A request by a data subject or lawful representative to have Personal Data deleted from the HIAS information assets should be granted when:
    i. the Personal Data were not processed in compliance with this Policy;
    ii. retention of the Personal Data would not be in compliance with this Policy;
    iii. in cases where the only legitimate basis for processing is consent, the data subject withdraws the consent on which the processing was based; or
    iv. a request has been granted to fully restrict processing as stipulated in subsection L., below.
b. Personal Data shall not be deleted in the following circumstances:
    i. there are overriding vital interests, beneficiary interests, legal obligations or other legitimate interests; or
    ii. HIAS is required to process further for statistical, historical or scientific purposes.
c. Records held in HIAS archives shall not be deleted in order to preserve the integrity of HIAS records.

L. Objection to and Restriction of Processing

a. Data subjects or lawful representatives may, at any time, object to or request restriction of the processing of their Personal Data if:

i. the processing would not be in compliance with this Policy;
ii. where the only legitimate basis for processing is consent, and the data subject withdraws the consent on which the processing is based; or
iii. on compelling grounds relating to their particular situation.

b. The request shall be granted unless there are overriding vital interests, beneficiary interests, legal obligations or other legitimate interests.

M. Portability

a. Data subjects or lawful representatives may, at any time, request to port their data to another organization unless the Personal Data is contained in unstructured format, in a HIAS archive, or where there are other extenuating circumstances.

N. Automated Decision-Making

a. Data subjects are entitled not to be subject to a decision based solely on automated processing which produces adverse legal or significant material effects on them, unless the processing is carried out with consent, is necessary for entering into or performance of a contract between the data subject and HIAS, or is necessary for beneficiary interests or other legitimate interests (and provided that appropriate safeguards are in place).

O. Personal Data Transfers

a. Transfers may only occur when there is a legitimate basis for both Personal Data transfer and data processing.
    i. What constitutes a legitimate basis has been set out in this Policy, and this legitimate basis applies equally to data processing and data transfers.
    ii. Each of the data protection principles and sections of this Policy applies equally to data processing and data transfers.

VII. Legal Obligations and Compliance

HIAS may disclose Personal Data or other information if required to do so by law or in the good-faith belief such action is necessary to comply with applicable laws, in response to a court

order, judicial or other government subpoena or warrant, or to otherwise cooperate with law enforcement or other governmental agencies, including our funders. HIAS also reserves the right to disclose Personal Data or other information in good faith, that is appropriate or necessary to (i) take precautions against liability, (ii) protect HIAS or others from fraudulent, abusive, or unlawful uses or activity, (iii) investigate and defend HIAS against any third-party claims or allegations, (iv) protect the security or integrity of HIAS staff and associated personnel, clients/beneficiaries or any facilities or equipment used, or (v) protect HIAS' property or other legal rights, enforce HIAS' contracts, or protect the rights, property, or safety of others.

VIII. Minor and Children's Privacy

HIAS staff and associated personnel must not knowingly collect Personal Data from children under the age of 13 without obtaining parental consent; for children aged 13 to 18, HIAS must comply with applicable laws and regulations regarding parental consent. If HIAS learns Personal Data has been collected on or from persons under 13 years of age and without verifiable parental consent, HIAS must take the appropriate steps to delete this information.

IX. Responsibilities

If HIAS staff and associated personnel have any concerns, requests or complaints about this Policy, or if a data subject has concerns about their Personal Data, contact, or refer the data subject to contact, as applicable, HIAS' DPO by email at dpo@hias.org or by mail as per below:

HIAS, Inc.
1300 Spring Street, Suite 500
Silver Spring, MD 20910
Attn: Director, Data Protection and GDPR

X. Changes and Updates to this Policy

HIAS reserves the right to make changes and updates to this Policy as required. If modified the Policy will be made available to all HIAS Staff and associated personnel and on HIASnet indicating the date of the latest revision, and HIAS will comply with applicable law.

ANNEX 1: DEFINITIONS

1. **Consent** means, in light of the information provided to the individual data subject, any freely given, specific and informed agreement of a data subject to the processing of their personal data.
2. **Controller** means the entity or individual, including a public authority, agency or other body, who, alone or jointly with others, determines the purposes and means of the processing of personal data.
3. **Data subject** means an individual whose personal data is subject to processing under this Policy, regardless of who provided the personal data or how it was found. For the purpose of the Policy, the term data subject includes but is not limited to past, potential or current staff, beneficiaries, individual donors, supporters or suppliers.
4. **Personal data** means any information relating to an identified or identifiable individual ('data subject'). An identifiable individual is one who can be identified, directly or indirectly, in particular by reference to i) an identifier such as a name, an identification number, audiovisual materials, location data, an online identifier, ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual or iii) assessments of the status and/or specific needs, such as in the context of assistance programs. The definition of what constitutes personal data is contextual and expanding particularly due to enhancements in technology and methods for identifying individuals.
5. **Personal data breach** means a breach of security leading to the accidental or unauthorized destruction, loss, alteration, disclosure, access, or unplanned loss of availability of personal data that is unencrypted or can be decrypted.
6. **Personal data transfer** means any action that makes personal data accessible or otherwise available to another party, other than the data subject, regardless of the media and format (electronically or physically). Personal data transfer includes transfers within a country as well as data transfers from the country where the data was originally collected to another country or countries.
7. **Process or processing** means any operation or set of operations performed on personal data, whether by automated means or manually, such as collecting, recording, structuring, consulting, retrieving, using, transferring, disclosing, sharing or otherwise making available, or deleting.

Headquarters 1300 Spring Street, Suite 500 • Silver Spring, MD 20910 • 301 844 7300 • hias.org
SILVER SPRING • NEW YORK • WASHINGTON DC • CARACAS • LESVOS • N'DJAMENA • NAIROBI • PANAMA CITY • QUITO • SAN JOSE • TEL AVIV • VIENNA

8. **Processor** means an individual or entity, including a public authority, agency or other body, which processes personal data on behalf of the controller.
9. **Sensitive personal data** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, criminal history, genetic data and biometric data capable of uniquely identifying a natural person, data concerning health, or data concerning an individual's sex life or sexual orientation.

Headquarters 1300 Spring Street, Suite 500 • Silver Spring, MD 20910 • 301 844 7300 • hias.org
SILVER SPRING • NEW YORK • WASHINGTON DC • CARACAS • LESVOS • N'DJAMENA • NAIROBI • PANAMA CITY • QUITO • SAN JOSE • TEL AVIV • VIENNA