9/14/2023

English

Country Name: Uganda

DPO.Uganda@ahf.org (mailto: DPO.Uganda@ahf.org?)
Plot 54 B
Kira Road,
Kampala Uganda

Personal Data Use and Protection Policy

Purpose:

To establish procedures to protect Personal Data and to ensure the rights of individuals who are owner of the Personal Data in accordance with applicable laws and regulations.

Definitions:

“AHF” means, as applicable, either AIDS Healthcare Foundation or an affiliated entity or division of AHF that operates in the country where this policy is being applied.

“Authorization” means prior, express, and/or informed consent of the Client to carry out use of the Client’s Personal Data.

“Consent” means any freely given, specific, informed and unambiguous indication of the Data Subject's wish which he or she, by a statement or by a clear affirmative action, signifies agreement to the collection or processing of Personal Data relating to him or her.

“Bureau” means the one of the following global regions, as indicated in any Country Annex: Africa Bureau, Asia Bureau, India Bureau, Europe Bureau, Latin America and Caribbean Bureau.

“Client” means any natural, legal, or juristic person, as applicable, including, without limitation, a patient, employee, or contractor of AHF and whose Personal Data is subject to Use.

“Data Controller” means either AHF or any authorized employee or contractor or collaborator of AHF who Uses or manages Use of Personal Data on behalf of AHF.

“Data Processor” natural person, legal person of private law or public entity that acting alone or jointly with another, performs the processing of personal data on behalf of the data controller, under a legal relationship that binds it with the latter and delimits the scope of its action. It includes whoever performs the processing without the existence of a personal databank.

“Data Protection Authority” means such governmental agency or office that has been authorized with oversight of compliance under Data Protection Laws.

“Data Protection Laws” means the applicable laws governing Personal Data in the jurisdiction where this policy is being applied as indicated in the applicable Country Annex.

“Data Recipient” means any Data Controller or Data Processor that receives Personal Data from AHF or its Data Controllers and Data Processors.

“Data Subject” means natural person to whom the personal data corresponds.

“Data User” means AHF or any authorized employee or contractor or collaborator of AHF that makes decisions with regards to Personal Data and / or the Processing of Personal Data.

“Database” means any organized set of Personal Data that is the object of Use;

"Personal Data" means any information linked or associated with one or more specific or determinable Client, which can include, without limitation, marital status, first and last name(s), date and place of birth, gender, nationality, address, email address, telephone number, professional position, IP address and any other information used to communicate with us.

"Use" means any use of or operation on Personal Data such as without limitation the collection, storage, circulation, processing, or suppression of Personal data performed by or on behalf of AHF in the applicable jurisdiction.

Scope and Applicability:

The principles contained in this policy generally apply to all Personal Data used in the operations of AHF, provided that the provisions contained in the applicable Country Annex attached hereto will apply in such country. In the event of any conflict between a Country Annex and this Policy, the Country Annex will control Use of Personal Data by AHF in that country.

Policy:

It is AHF's policy to:

1. Protect and safeguard the Personal Data of Clients;
2. Inform Clients of their rights with regards to their Personal Data;
3. Maintain and update Personal Data;
4. Adopt and compile policies and procedures to ensure compliance with Data Protection Laws;
5. Process complaints and claims of Clients regarding Personal Data; and
6. Complying with the instructions and requirements of regulatory agencies that have jurisdiction over AHF with regards to Personal Data under the Data Protection Laws.
7. Where required by the Data Protection Laws, register AHF with the applicable Data Protection Authority.

AHF may collect Personal Data of Clients in situations including, without limitation:

1. When a Client registers on our Website,
2. When a Client fills in one of our forms,
3. When a Client signs any contract with us,
4. When a Client subscribes to our newsletters and announcements.

Procedures:

1. Each AHF Affiliate must enter into a written contract with each third party Data User or Data Processor such that:
    a. The third party's roles, responsibilities, and obligations with respect to Personal Data are clearly identified;
    b. The third party expressly commits to safeguarding Personal Data, immediately notifying AHF of any breaches of Personal Data, and taking all necessary steps to mitigate any harm to Personal Data or to the Clients arising out of any breach of Personal Data;
    c. The third party indemnifies and holds the AHF Affiliate harmless from any failure of the third party's obligations under the contract.
2. AHF and its Data Recipients shall have the same obligations with regards to Personal Data. For this purpose, AHF will:
    a. Ensure that Personal Data provided to Data Recipients are correct;
    b. Communicate updates regarding Personal Data to Data Recipients;
    c. Require that Data Recipients protect Personal Data;
    d. Process queries and claims;
    e. Inform the Data Recipients when any Personal Data of a Client is under discussion;
    f. Provide to Data Recipients only the Personal Data whose Use is authorized;
    g. Inform Clients of their rights and about the Use of their Personal Data; and
    h. Inform applicable Data Protection Authority of violations of safeguards that are intended to protect Personal Data and any risks in information management that endanger Personal Data.
3. Additionally, AHF will:
    a. at the time it requests authorization from the Client, clearly and expressly inform the Client of the following:
        i. The Use to which the Client's Personal Data will be subjected to and the purpose of the Use and any possible third-party users or types of uses;
        ii. Whether the responding to the requested information is mandatory or optional; whether the any request information containing sensitive data of children and adolescents are optional; and the consequences of refusing to provide information or providing false information

iii. The rights that assist the Client and the mechanism to exercise those rights; and the possibility to file a complaint before the data protection authority of the country of residence of the data subject.

iv. The identification (i.e. physical or electronic address and telephone number) of AHF.

b. keep proof of compliance with the provisions of Data Protection Laws and when requested by the Client, provide a copy of such proof;

c. guarantee the Clients, at all times, the full and effective exercise of the rights with regards to their Personal Data;

d. request and keep a copy of the respective authorization granted by the Client in accordance with the Data Protection Laws;

e. duly inform Clients about the purpose of Personal Data collection and their rights with regards to any authorization granted to AHF;

f. keep all Personal Data under the necessary security conditions in order to prevent the adulteration, loss, query, or fraudulent or unauthorized use or access;

g. ensure that Personal Data provided to any Data Controller is true, complete, accurate, updated, verifiable, and understandable;

h. update Personal Data, timely communicate to all Data Controllers any amendments to Personal Data provided by Clients, and take other necessary measures to maintain and update Personal Data;

i. amend and correct Personal Data when it is incorrect, and communicate the pertinent corrections and amendments to each affected Data Controller;

j. provide to the Data Controllers only the Personal Data whose Use is authorized by Data Protection Laws;

k. require the Data Controllers to respect the security and privacy conditions of the Client's Personal Data at all times;

l. process all queries and claims related to Personal Data in accordance with the Data Protection Laws;

m. implement internal procedures for inquiries and complaints related to Personal Data;

n. inform each Data Controller when certain Personal Data is under discussion by the Client, once a claim has been filed and the respective claim procedure has not been followed;

o. inform the Client, at the Client's request, about the Use of Client's data;

p. inform the appropriate Data Protection Authority of any breaches of security or other risks to Personal Data;

q. comply with the instructions and requirements issued by the Data Protection Authority.

4. Each third-party Data Controller must contractually agree to:

a. guarantee the Client, at all times, the full and effective exercise of Client's rights with regards to Personal Data;

b. keep Personal Data under the necessary security conditions in order to prevent the adulteration, loss, query, or fraudulent or unauthorized use or access;

c. timely update, rectify, or delete Personal Data in accordance with the terms of the Data Protection Laws;

d. update Personal Data reported by AHF within 5 business days from its receipt;

e. process the queries and claims made by the Clients in accordance with the Data Protection Laws;

f. adopt an internal manual of policies and procedures to ensure adequate compliance with the Data Protection Laws, paying special attention to inquiries and complaints by the Clients;

g. record in Personal Database the legend, "claim in process" or similar annotations in the form and manner required under the Data Protection Laws;

h. insert in Personal Database the legend, "information in judicial discussion," once notified by the competent authority on legal proceedings related to any Personal Data;

i. refrain from circulating Personal Data that is being disputed by the Client and with regards to which the Data Collector has received a restriction request from the Data Protection Authority;

j. allow access of information only to those who are authorized to access it;

k. inform the Data Protection Authority when there are violations of security codes and risks in the administration of Personal Data of the Clients; and

l. comply with the instructions and requirements by the Data Protection Authority.

5. For each jurisdiction, and as required by applicable Data Protection Laws, AHF will:

a. Designate a Data Protection Officer;

b. Publish a notice of its Person Data Use practices; and,

c. Establish and publish a policy for its Web based Use of Personal Data.

d. Permit Clients and their successors to query the Client's Personal Data that rests on any Database, whether from the public or private sector. For this purpose, AHF and each Data Controller must provide all of Personal Data contained in the individual record or that which is linked to the identification of the Client in accessible Databases. AHF or Data Controller may formulate the means of such query, as long as sufficient proof of the query is kept.

Local Supplement: Uganda

This Local Supplement is applicable to you if you reside in the country indicated above. It contains important information about your personal rights to privacy. Whenever this Local Supplement applies it should be considered to add to the Privacy/Data Use and Protection Notice.

"AHF" means **AHF Uganda Cares, Ltd.**, non-governmental organization duly incorporated and existing under the laws of Uganda.

"Data Protection Law" means Data Protection and Privacy Act, 2019 ("DPPA").

"Data Protection Authority" means the National Information Technology Authority-Uganda ("NITA Uganda").

Procedures

1. "Consent" means _____.
2. "Data Processor" means either Party to the extent that that Party manages or processes Personal Data under these DP Terms an "operator" as defined in the Data Protection Laws.