African Population and Health Research Center

Data Protection Notice in accordance with the

EU General Data Protection Regulation (GDPR)

The African Population and Health Research Center (APHRC) is an independent, 501(c) non-profit international organization committed to conducting high quality and policy-relevant research.

APHRC is committed to protecting the privacy and security of your personal information.

This data protection notice describes how we collect and use personal information about you before, during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).

APHRC is responsible for deciding how we hold and use personal information about you. This notice explains what personal data APHRC holds about you, how we share it, how long we keep it and what your legal rights are in relation to it.

This notice applies to you as a staff member of a grantee or partner organisation with whom APHRC is liaising. This notice does not form part of any contract or agreement. We may update this notice at any time as we deem fit.

It is important that you read this notice, together with any other data protection and privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles

APHRC will comply with GDPR which provides that the personal information we hold about you shall be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

African Population and Health Research Center

The kind of information we hold about you:

Personal data, or personal information, means any information relating to you as a living individual from which you can be identified. It does not include data where the identity has been removed (anonymous data)

There are "special categories" of more sensitive personal data which require a higher level of protection. These data include genetic, biometric and health data.

The categories of personal information that we may collect, store, and use about you include (but are not limited to):

- The contact details that are provided to us, including names, titles, addresses, telephone numbers and email addresses.
- Personal details/data such as gender, marital status, signatures etc.
- Financial information, such as salary information.
- Passport information or other travel related information
- Photos in your capacity as a staff member of a donor, grantee/partner organisation.
- Usernames and social media identity information in your capacity as a staff member of grantee/partner organisations.

We will, during the application process and throughout the agreement period, also collect, store and use the following “special categories” of more sensitive personal information:

- Details of any criminal allegations relevant to our relationship with your organisation.
- An assessment of creditworthiness of a person or an estimate of work performance by an employer.

African Population and Health Research Center

How is your personal information collected?

We typically collect your personal information through the application process, directly from you or individuals working for the donors, grantee/partner or from information which the grantee/partner has made publicly available.

We will collect additional personal information in the course of programme related activities throughout the period of the application process and the duration of any agreement period.

How we will use information about you

We will use your personal information as follows:

Purpose	**Legal Basis**
To produce and carry out our obligations under your agreement with us.	For the legitimate interests of administering our agreements and programmes with you.
To carry out grantee/partner audits.	For the legitimate interests of ensuring the funds provided to you are used as expected and required.
To make payments and processing payment information request forms/invoices.	For the legitimate interests of APHRC to be able to administer our agreements and programmes with you.
To carry out due diligence on grantees/partners.	For the legitimate interests of assessing projects before offering or committing to providing funds to you.
To make external press releases (including website updates, e-blasts) or internal communications.	For the legitimate interests of APHRC in connection with demonstrating the projects that APHRC support and help to deliver.
To review agreements and programme budgets.	For the legitimate interests of APHRC in connection with understanding and approving how funds will be used.

To arrange meeting with donors, grantees/partners.	For the legitimate interests of APHRC in connection with administering the agreements and discussing potential new projects/progressing agreements and payments.
To carry out workshops/training/other networking	For the legitimate interests of APHRC in connection with developing the organisational capacity of grantees/partners
To arrange travel/visa's for grantees/partners	For the legitimate interests of APHRC in connection with assisting grantees/partners to travel for the purposes of relationship building and administering the agreements

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

In a small number of cases where other lawful bases do not apply, we will process your data on the basis of your express consent.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the agreement we have entered with you or we may not be able to carry out the required due diligence in order to take the project forward and assess the possibility of entering an agreement with you.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Criminal convictions and allegations of criminal activity

Further legal controls apply to data relating to criminal convictions and allegations of criminal activity. We may process such data on the same grounds as those identified for "special categories" referred to above.

Do we need your consent?

We do not need your consent to process your personal information if the processing is carried out for legitimate legal interests. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your agreement with us that you agree to any request for consent from us. You are also at liberty to withdraw your consent at any time.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.

2. Where it is necessary to perform the agreement with you and appropriate measures are in place to safeguard your rights.

3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Data sharing

We do not, and will not, sell your data to third parties.

We may have to share your data with third parties, including third-party service providers.

We require third parties to respect the security of your data and to treat it in accordance with the law.

African Population and Health Research Center

Why might you share my personal information with third parties?

We may share your personal information with third parties where required by law, where it is necessary to administer the contractual relationship with you or where we have another legitimate legal interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including consultants).

Examples of bodies to whom we may voluntarily disclose data, in appropriate circumstances, include but are not limited to:

Organisation	**Justification**
Agencies with responsibilities for the prevention and detection of crime, apprehension and prosecution of offenders, or collection of a tax or duty, and other regulatory agencies.	For the prevention, detection or investigation of crime, for the location and/or apprehension of offenders, for the protection of the public, to support national interest and/ or to comply with regulatory requirements.
Third party service providers.	To facilities activities of APHRC including activities that are carried out by third-party service providers, including auditors, insurance companies, travel/courier companies, training providers, banks, professional advisors such as law firms, IT services, media/communications agencies, event venues/organisations, payment providers. Any transfer will be subject to an appropriate, formal agreement between APHRC and the third party service provider.

Where information is shared with third parties, we will seek to share the minimum amount of information necessary to fulfil the purpose.

How secure is my information with third-party service providers?

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes (as written in the contract between us) and in accordance with our instructions.

What about other third parties?

We may share your personal information with other third parties. We may need to share your personal information with a regulator or to otherwise comply with the law.

Data security

> We have put in place measures to protect the security of your information. Details of these measures are available upon request.
>
> Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business requirement to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Sharing your data outside the European Union

APHRC has office registrations in Kenya and Senegal. APHRC may share your personal information with other colleagues within the branch offices. All employees of APHRC are under an obligation to handle data in accordance with the data protection policy and with the protections of GDPR.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Retention periods may increase as a result of legislative changes, e.g. an increase in limitation periods for legal claims would mean that APHRC is required to retain certain categories of personal data for longer.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. We may keep anonymised statistical data indefinitely.

African Population and Health Research Center

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Suspend processing of your personal information**, for example if you want us to establish the accuracy of the data we are processing.
- **Object to any direct marketing** (for example, email marketing or phone calls) by us, and to require us to stop such marketing.
- **Object to any automated decision-making** about you which produces legal effects or otherwise significantly affects you.
- **Request the transfer** of your personal information to another party.

Please be aware that these rights are subject to certain conditions and exceptions as set out in the data protection legislation.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Officer in writing and they will explain any conditions that may apply.

No fee required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights).

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where we are relying on your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Officer. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Changes to this data protection notice

We may need to update this notice from time to time, for example if the law or regulatory requirements change, if technology changes or to make APHRC's operations and procedures more efficient. If the change is material, we will give you not less than two months' notice of the change so that you can exercise your rights, if appropriate, before the change comes into effect. We will notify you of the change by email.

Data Protection Officer - Contact Details

If you need to contact us about your data, please contact Paul Odero podero@aphrc.org

Date: May 24, 2018