

Request for Expression of Interest

|  |  |
| --- | --- |
| **DATE: 07/04/2022** | **FROM: Malaria Consortium Abuja** |
| **CONTACT: No 33 Pope John Paul Street, Off Gana Street, Maitama Abuja, Nigeria**  |

**Request for NITDA licensed Data Protection Compliance Organization services for the provision of annual privacy and data protection practices audit to Malaria Consortium**

Malaria Consortium is one of the world's leading non-profit organizations dedicated to the comprehensive control of malaria and other communicable diseases in Africa and Southeast Asia. Malaria Consortium works with communities, government and non-government agencies, academic institutions, and local and international organizations, to ensure good evidence supports delivery of effective services, providing technical support for monitoring and evaluation of programmes and activities for evidence-based decision-making and strategic planning. The organization works to improve not only the health of the individual, but also the capacity of national health systems, which helps to relieve poverty and support improved economic prosperity.

Malaria Consortium supports multiple projects in Nigeria with different projects starting and ending each year, as such our demand for supplies and services nationally and internationally varies year on year. The majority of Malaria Consortium supply and service needs are procured locally in our countries of operation where the right price and quality can be obtained. Internationally sourced products predominantly include pharmaceutical and medical items, with other small ad hoc needs on rare occasions (including vehicles). For the purpose of business Malaria Consortium also has a registered Nigerian entity known as Malaria and Public Health Nigeria ltd/GTE.

**Rationale**

According to the Nigeria Data Protection Regulation, every organization in Nigeria is required to conduct Data Privacy Audits once annually and a report of the conducted audit be submitted to the National Information Technology Development Agency (NITDA), Malaria Consortium is thus looking for registered Data Protection Compliance Organization to conduct an annual privacy and data protection audit service.

**Objective of the Service request**

Conduct an annual privacy and data protection audit service in line with industry standards and best practices per Nigeria regulatory guidelines ensuring quality delivery.

**Key activities for the Service Provider**

Key activities include:

1. Compliance audit and report filing:
	1. Conduct an audit of the organisation’s privacy and data protection practices for the year 2021;
	2. Submit a summary of the audit containing information as stated in 4.1(5) of NDPR 2019 to the National Information Technology Development Agency (NITDA);
2. Remediation support
	1. Prepare and present a remediation plan to remediate identified noncompliance
3. Data Protection Impact Assessment
	1. Evaluate the status of data protection compliance
	2. Identify nonconformity and non-compliance risks in the organization before filing
	3. Provide suggestion of mitigating actions against the identified risks
4. Training and capacity development
	1. Assess the level of awareness of top management in respect of NDPR Compliance practice and training

Expected Output/deliverables

1. Assessment review and identification of all processes that transact on personal data in the agency
2. Reviewed existing control system and provide report on its level of compliance with the NDP Regulation
3. Assessment of all third party engagement and controls around the protection of personal data
4. Preparation of management report with respect to the data audit findings
5. Provision of necessary recommendations along with a timeline geared towards bridging the gaps that are not compatible with the data protection regulation
6. Where necessary provide advice on the set up of a data protection unit within MC
7. Submission of exception report to the management highlighting possible data breach points that could compromise personal data and associated remedial actions
8. Develop a data privacy policy framework for the activity within Nigeria

**Profile requirements for the Service Provider**

1. The Data Protection Compliance auditor should be a licensed qualified data audit organization with National Information Technology Development Agency (NITDA)
2. The licensed Data audit organization should have at least five (5) years experience related to vast audit exercises and at least two (2) years related to Data protection audit

**Requirements for selection**

Interested firms are required to submit EOI prepared in English Language with the following requirements which shall be used as criteria for preliminary selection.

**Mandatory (Without which companies will be disqualified)**

(i) Evidence of registration with Corporate Affairs Commission.

(ii) Proof of tax remittance (Tax Clearance Certificate) for the last three years

(iv)Proof of VALID license with NITDA

**Required Documents for Selection**

The Service Provider shall submit the following in addition to the Mandatory requirements, but not necessarily be limited to:

1. Proof of relevant experiences- Demonstrated service delivery capacity for Data protection audit services for similar Non-Governmental Organizations (NGOs) and non-profit organizations within the last two years (2020-2021).
2. Include information on your capability of providing quality audit services -Question 1 of the BRD
3. Proof of past experience by provision of 3 contracts/P.O’s from similar Non-Governmental Organizations (NGOs) and non-profit organizations
4. Fully Complete information in below Annex and Bidder Response Document attached to the EOI
5. Positive Reference letter from not less than three similar clients (INGOs, public health).

**EOI Submission**

Applications for EOI accompanied by the relevant documents should be sent by email to tenders@malariaconsortium.org only, within the stipulated timeline for submission.

Malaria Consortium will not be accepting hard copies of any documents at this time due to relevant COVID protocols

**Closing Date**

All submissions must be received at the above Office or tenders’ box not later than 27th of April 2022

**Important Notice**

* *Only short-listed firms will be contacted*
* *The company reserves the right to reject any response to this request for EOI.*

**Malaria Consortium**

Malaria Consortium is committed to fair and competitive procurement processes, and all expression of interests received will be considered confidential, and will not be shared with other bidders.

* Any inappropriate action to influence the award including personal incentives to Malaria Consortium staff is prohibited.
* Any discounts or cost reductions must be included in the original quote to be considered.

For more information or question(s), you can send it as an email to tenders@malariaconsortium.org before close of business on 20th April 2022 at 5pm WAT

Thank you for your review of this information.  We look forward to hearing from you.

**ANNEX 1:**

**Malaria Consortium –**

**Pre-qualification Subissions Document for all Bidders**

**NOTE: All information provided will be subject to verification and service providers will be disqualified and blacklisted if any provided information is found false**

|  |
| --- |
| **About you and your bid** |
| **Service applied for** |  |  |
| **Company Name** |  |  |
| **Company Address and Contact** |  |  |
| **Your Name***(the person filling the form)* |  |  |
| **Please state clearly any relationships you may have with MC staff?****Friends/Family/Business partners etc.***(Failure to name such relationships will invalidate this bid.)* |  |  |
| **About your company?** |
| **How long has the company been formed?** |  |  |
| **Is the Business incorporated? Please enclose CAC** |  |  |
| **Please enclose details of the company bank account if you have one and Tax Identification Number** |  |  |
| **Please give the names of the company owners?**  |  |  |
|  |  |  |
| **About your experience/skills providing these goods/services?** |
| **What experience do you have of supplying this items/service previously?***Give details* |  |  |
| **Have you provided similar service to other NGO’s in Nigeria?****Who? /What kind of Service?** *Attach proof* |  |  |
| **Have you provided services to Malaria Consortium?** *Please give a brief summary* |  |  |
| **What expertise do you have concerning the items/service you are bidding to supply?****Do you hold any relevant qualifications in this area?** |  |  |
|  |
| **Standard payment terms: 30 days payment after delivery Is this acceptable to you?** |  |  |
| **Is it acceptable for us to visit your office/premises?** |  |  |
| **Give name of 2 business referees and detail of business undertaken?** *(Someone you have supplied goods / provided service to in the last year, preferably work of a similar nature)* |  |  |
| **Signature, Date and Company Stamp** |  |  |

**Anti-Bribery Policy**

1. **Purpose and context**

Malaria Consortium’s policy is to conduct its work in an honest and ethical manner. Malaria Consortium, wherever it operates, takes a zero-tolerance approach to bribery and is committed to ensuring that its employees act professionally, fairly and with integrity in all dealings wherever Malaria Consortium operates. This is to ensure that the organisation benefits from a valued reputation, and donor and partner and beneficiary confidence.

1. **Principles**

Malaria Consortium is committed to implementing and enforcing effective systems to counter bribery.

1. **Scope**

This policy applies to all individuals in the organisation, including trustees, senior managers, employees (whether permanent, fixed term or temporary), volunteers and interns, consultants, partners and any other person or organisation providing services to Malaria Consortium whether paid or unpaid.

All employees will be trained on this policy on joining the organisation as part of their finance induction. They will be asked to sign that have read, understood and agree to abide by its content. All other persons associated with the organisation will be informed of this policy through their contractual arrangements. For existing employees and associated persons, the policy is to be communicated via the Country Director, the Regional Programmes Director in the regions and the Financial Controller in each country.

1. **Definition and terms**

What is a bribe?

A bribe is a financial or other advantage offered or given:

* To anyone to persuade them to or reward them for performing their duties improperly or;
* To any public official with the intention of influencing the official in performance of their duties. This includes any form of gift or payment to an official in an attempt to speed up or complete a process quicker than usual. The size of the gift is irrelevant.
1. **Implementation**

Any individual suspected of offering, promising or giving a bribe, requesting, agreeing to receive or accepting a bribe or bribing a public official will be investigated under the organisation’s disciplinary policy and if found guilty will be dismissed for gross misconduct. For any contractor found to offer, promise or give a bribe or requested or agreed to receive or accept a bribe or bribing a foreign public official, will have their contract terminated immediately, all business dealings will cease and financial compensation will be sought and it will be reported to the authorities as required by the Act.

If any individual is confronted with a request to make a bribe, individuals are to present a copy or explain this Anti-Bribery Policy and must not agree to the bribe in any circumstances. All vehicles should carry a copy of the policy for this purpose.

**Gifts and hospitality**

This policy does not prohibit the giving and receiving of promotional gifts of low value and normal and appropriate hospitality. Low value gifts are defined as those below GBP 5.00 or currency equivalent. Gifts and hospitality may amount to bribery; therefore, these must not be offered or given with the intention of persuading anyone to act improperly or to influence a public official in the performance of his duties. Any gifts or hospitality offered must be reported to the Country Finance Manager before acceptance and instruction given to the individual on whether or not the gift is to be accepted.

Any offer or promise must be documented, whether it is approved or not by the Country Finance Manager on the register of interest and gifts for the country. Malaria Consortium does not give out gifts, although within projects, some activities, such as low-cost incentives to voluntary workers, may be acceptable. These must be within the original project and its budget as agreed with the donor.

The register will be accessible by the Country Director, internal and external auditors and to regional and HQ staff performing checks on visits to the country.

**Facilitation payments and kickbacks**

Malaria Consortium does not make, and will not accept, facilitation payments or “kickbacks” of any kind. Facilitation payments are typically small, unofficial payments made to secure or expedite a routine government action by a government official, for example to clear goods or persons through customs. Kickbacks are typically payments made in return for a business favour or advantage, for example, to reduce delivery time on goods and services. All employees must avoid any activity that may lead to, or suggest, that a facilitation payment or kickback will be made or accepted on behalf of Malaria Consortium.

**Donations**

Malaria Consortium does not make contributions of any kind to political parties.

**Financial Systems**

Malaria Consortium will keep financial records and ensure appropriate internal controls are in place to ensure there is an evidence trail for any payments made to third parties, in order to prevent corrupt payments taking place.

All expense claims relating to hospitality, gifts or expenses incurred to third parties must be submitted in accordance with the financial procedures and must specifically record the reason for the expenditure.

All accounts, invoices, memoranda and any other documents and records relating to dealings with third parties, such as clients, suppliers and other business contacts, must be prepared and maintained with strict accuracy and completeness. No accounts must be kept “off-book” to facilitate or conceal any payments.

**Whistle Blowing**

Employees are encouraged to raise concerns about any issue or suspicion of malpractice at the earliest possible stage in accordance with Malaria Consortium’s Whistle Blowing Policy. Malaria Consortium will apply criminal and administrative sanctions in a robust manner to demonstrate a zero tolerance to bribery.

**Monitoring**

The effectiveness of this policy will be regularly reviewed by the Board of Trustees and internal control systems and procedures will be subject to audit under the internal audit

**Anti-Fraud and Anti-Corruption Policy**

1. **Purpose and context**

The aim of Malaria Consortium’s fraud and anti-corruption policy is to minimise fraud through a series of measures, including clear policies and processes, regular internal and external audits and training for all staff.

1. **Principles**

Malaria Consortium is committed to investigate any and all suspected acts of fraud, misappropriation or other similar irregularity. Detecting fraud and corruption is everyone’s responsibility and if any incident or potential incident is discovered staff must report it immediately, as required by Malaria Consortium’s whistle blowing policy.

1. **Scope**

Malaria Consortium is committed to maintaining an untainted reputation with its donors, partners, beneficiaries and vendors. All Malaria Consortium employees and Suppliers are under obligation to maintain integri­ty in all actions and must avoid circumstances that compromise their decisions or actions. All employees must ensure that the ethical business practices and interests of the organisation are observed.

It is a major violation of Malaria Consortium’s policies for employees or Suppliers to knowingly conceal, falsify or misrepresent a material fact relating to any transaction. Misrepresentation may include but is not limited to: signing for receipt of goods or services not yet received or completed, or altering any document to disguise or change the outcome, including the back-dating of documents. For employees proven violations will lead to disciplinary action up to dismissal from employment and legal action. For Suppliers proven violations will result in the immediate termination of their contract and the cessation of all business dealings.

1. **Definition and terms**

Fraud is defined in the Uganda Act, as false representation, failure to disclose information or abuse of position, in order to make a gain for yourself or another or to cause or expose another to a risk of loss. Fraud covers an act of deception, bribery, forgery, extortion, theft, misappropriation, false representation, conspiracy, corruption, collusion, embezzlement, or concealment of material facts.

Anti-corruption: relates to the measures taken to eradicate or prevent dishonest or fraudulent conduct.

Both corruption and fraud amount to abuse and theft. Acts of fraud and corruption include, but are not restricted to:

* Falsifying time sheets or payroll records
* Falsifying travel and entertainment expenses
* Fictitious reporting of receipts from suppliers or shipments to customers
* Creation of false invoices or purchase orders, including the back-dating of documents
* Misappropriation of Malaria Consortium and donor equipment, resources and even data
* Misstatement of income
* Misstatement of assets
* Understatement of liabilities
* Paying bribes, that is payment to another person to induce a certain action from them, this includes payments to officials such police officers requesting unofficial payments on road blocks
* Receiving money or gifts in order to undertake a certain action for example ordering with a specific supplier
* Obtaining Malaria Consortium income or assets by deception
* Claiming to provide services to beneficiaries that do not exist, and other forms of identify fraud

**5. Implementation**

Steps to mitigate occurrence

The organisation adopts the following anti-fraud measures to minimise its risk from fraudulent activity:

* Clear policies on the expected conduct of staff in the organisation, for example Anti-Bribery and Code of Conduct communicated as part of induction programme and updates staff in team meetings.
* Records and investigates all incidences including suspected and confirmed fraud, in line with MC Guidance on Conducting a Fraud investigation.
* Reports fraud to the police and to the Charity Commission.
* Implements robust controls and informs staff about the procedures and measures in place.
* Ensures records of all income and expenditure are kept and receipts, invoices and supporting documents are adequate.
* Checks that financial controls are not overridden, by-passed or ignored
* Reconciles bank accounts monthly and conducts spot checks
* Uses tiered delegated authority and signature levels for all payments
* Restricts and closely monitors access to sensitive information
* Implements an Internal Audit function reviewing processes and procedures on a risk basis
* Establishes clearly defined roles for staff that include segregation of duties

Malaria Consortium has a zero tolerance to fraud and corruption. Malaria Consortium will apply robust sanctions to combat fraud and corruption including disciplinary action and reporting suspected criminal activity to the police.

**Safeguarding Policy**

**1 Purpose and context**

Malaria Consortium works with communities, governments, academic institutions, and local and international organisations, to ensure effective delivery of services. Our work often puts those that work for us in position of power in relation to children & adults in vulnerable circumstances in the communities that we work with and we have an obligation not to abuse this power and to actively act against any such abuse. Our capacity to ensure the protection of children & adults in vulnerable circumstances depends on the ability of staff and partners to uphold and promote the highest standards of ethical and professional conduct.

Malaria Consortium has a strong commitment to the welfare of all beneficiaries and their protection from harassment abuse and exploitation to provide safeguards in all of our work with communities. Children and adults in vulnerable circumstances in those communities can be at particular risk and, it is a collective responsibility to prevent abuse and exploitation.

In recognising our responsibility to protect children and adults in vulnerable circumstances from any harm that may be caused due to their coming into contact with the organisation, Malaria Consortium has developed a Safeguarding Policy, which outlines this commitment and its implications. This policy sits within a policy and governance framework that is underpinned by our values, what we stand for and intend to achieve. We aim to identify and minimise risks, deter and remove opportunities for abuse to occur. This is done by upholding high standards and putting in place stringent mechanisms to monitor these and learn from the past.

Policy Framework

Quality monitoring evaluation, quality assurance, learning

Reporting and responding: to concerns and grievance, whistleblower, desciplinary

Policy and Practice:

Recruitment, induction, bullying and harrassment,

sexual harrassment, health and safety, equal opportnities and diversity, dignity at work, human

trafficking, safeguarding and child protection,

Our Standards:

Code of Conduct, Supplier/ Partner Code of Conduct, Risk

Management

Who we are:

Purpose, values, goals, governance

This policy is aligned with general international standards including the United Nations Convention on the Rights of the Child. The Organisation will comply with laws relating to human trafficking as set out in our [Modern Slavery Statement.](https://www.malariaconsortium.org/who_we_are/modern-slavery-statement.htm) While Malaria Consortium staff and partners will comply with local legislation, if the standards outlined in this policy are stronger than local legislation, then this policy is to be followed.

**2 Principles**

The Safeguarding Policy is committed and guided by the following set of principles:

**2.1 Mandatory Compliance**

Malaria Consortium staff members and partners must ensure they understand the Safeguarding Policy,

their responsibilities and how to report any wrongdoing or concerns. This policy are mandatory for all

Malaria Consortium staff and partners and no exceptions will be made.

Malaria Consortium complies with reporting requirements from donors and relevant bodies on Safeguarding and Human Trafficking concerns.

**2.2 Upholding of Protection Rights**

• All children and adults in vulnerable circumstances have equal rights to protection from harm. They should be empowered to understand their rights in this area, and made aware of what is acceptable and what they can do if there is a problem or concern.

• Everybody has a responsibility to support the protection of children and adults in vulnerable circumstances.

• Organisations have a duty of care to children and adults in vulnerable circumstances with whom they work, are in contact with, or who are affected by their work and operations.

• If working with partners, organisations have a responsibility to help any partner meet the minimum requirements on protection.

• The Human Rights of children and adults in vulnerable circumstances will be respected and everyone the organisation comes into contact with will be treated with respect and dignity regardless of age, disability, gender, civil status, race, religion or belief; gender and sexual orientation.

• No form of discrimination, harassment, or abuse (physical, sexual or verbal), intimidation or exploitation is acceptable.

• The best interests of the child or adult in vulnerable circumstances will guide safeguarding decisions.

**2.3 Zero Tolerance to Inaction**

• Malaria Consortium operates a zero tolerance approach to abuse and exploitation. Under no circumstances will any abuse by Malaria Consortium staff and partners be tolerated, and all concerns will be investigated without delay, and each case will be dealt with fairly and professionally and referred to local authorities if required.

• The organisation is open and transparency. Safeguarding concerns will be raised and discussed, poor practice and inappropriate behaviour will be challenged and addressed, and safeguarding measures will be continuously reviewed and strengthened to ensure the organisation remains accountable to children and adults in vulnerable circumstances.

• Managers have a particular responsibility to uphold the highest standards, to set a good example, and to create a working environment that supports and empowers staff. They have a responsibility to understand and promote the policy. They must do all they can to prevent, report and respond appropriately to any concern or potential breaches of the policy.

• Zero tolerance of inappropriate behaviour applies whether a proven incident happens in or out of working hours.

• Malaria Consortium safeguarding approach prevails in all the stages of our operations, projects and activities, thus ensuring the organisation does not harm children and adults in vulnerable circumstances.

**3 Scope**

The policy applies to all staff members and partners. In this policy ‘staff members’ and ‘staff’ are taken to refer to all internal staff and ‘partners’ is taken to refer to all trustees, consultants, contractors, volunteers, interns, partner agencies, sub-grantees, community workers, suppliers and visitors to projects.

**4 Definitions and terms**

The following definitions will be used throughout the policy.

**Child:** This policy regards a child as anyone under the age of 18 years, irrespective of alternative local definitions.

**Protection**: Protection includes ensuring that individual basic human rights, welfare and physical security are recognised, safeguarded and protected in accordance with international standards.

**Safeguarding:** Safeguarding is the combination of policies and actions undertaken to protect children and adults in vulnerable circumstances by mitigating risks, responding to and referring cases, to ensure no harm as a result of association with the organisation.

**Sexual exploitation:** Is the abuse of vulnerability, differential power, or trust for sexual purposes; this includes profiting monetarily, socially or politically from the sexual exploitation of another. Prostitution, human trafficking for sexual abuse, modern slavery and exploitation are only some examples of this.

**Adult in vulnerable circumstances**: Is defined as someone over the age of 18 unable to take care of themselves / protect themselves from harm or exploitation; or who, due to their gender, mental or physical health, disability, or as a result of disasters and conflicts, are deemed to be at risk of being abused.

**5 Implementation**

Malaria Consortium will work to reduce the risk of abuse and exploitation of children and adults in vulnerable circumstances by staff members and partners by following the procedures outlined below.

**5.1 Prevention**

**5.1.1 Risk Assessment and Programme Design**

Malaria Consortium will assess safeguarding risks at three levels one at the role level, one at the programme design level and one for suppliers.

**Role Level**

As part of Malaria Consortium’s job evaluation process following role design and prior to recruitment every role is assessed for its inherent risk to Safeguarding. This is done by the recruiting manager and Human Resources. This risk level is then validated by the job evaluation committee against other similar roles across the organisation and checked for local contextual factors. Once this is complete the role safeguarding risk level is included on the job description and the employee record in the HR Information System.

The Human Resources Director is responsible for ensuring that all job descriptions reflect the level of risk for each role following the job evaluation process and the Country or Regional Directors are responsible for ensuring all staff have agreed mitigating actions and that they are completed.

**Programme/ project Level risk assessment**

Malaria Consortium will design programmes in a way which takes into account potential risks to children and adults in vulnerable circumstances, and act to minimise any identified risks. Risks can be intended or unintended, and can be from Malaria Consortium staff, volunteers, vendors, or others associated with the organisation. Risks can also be incidental, such as an activity in which mothers are expected to leave their children at home unattended.

Malaria Consortium incorporates safeguarding into any standard risk assessment it conducts when designing a new project. All projects will be assessed during the design phase for their potential risks to children and adults in vulnerable circumstances, and mitigation strategies developed. Project managers will be responsible for conducting a safeguarding risk assessment for each of their projects, and ensuring the policy is implemented at all times.

The respective Country Director is responsible for signing all project safeguarding risk assessments as proof that it been reviewed and sending them back for filing in the relevant project folder(s). The Country Director will also ensure all high level risks are flagged through the regional risk register to the corporate register if applicable and all medium and low risks are to be monitored by programme and regional management levels.

**Supplier**

Malaria Consortium requires all suppliers contracted directly by Malaria Consortium, nationally or internationally, to agree to our Procurement Terms and Conditions, including our ethical standards.

Malaria Consortiums Procurement Terms & Conditions, ethical standards (section 3.1): “The Supplier shall observe the highest ethical standards during the performance of its obligations under this Contract including international labour standards promoted by the International Labour Organisation, including in the areas of child labour and forced labour”

Malaria Consortium will also check all suppliers from whom Malaria Consortium procures

supplies or services nationally or internationally, against international sanctions and vetting lists which, amongst other details, include persons or entities that are convicted of engaging in or supporting sanctioned activities, including human trafficking. Malaria Consortium will not procure from any suppliers on international sanctions and vetting lists.

**5.1.2 Recruitment and Selection**

The organisation has guidelines in place covering the recruitment process of all staff. The recruitment guidelines will be reviewed and updated regularly to ensure that they accurately reflect ‘safe recruiting’ and screening standards.

**5.1.3 Checks**

Malaria Consortium expect all suppliers to conduct security checks such as references and police checks as part of their recruitment processes.

**5.1.4 Induction and Training**

Malaria Consortium expect all suppliers to include safeguarding training as part of their induction programme and refresher trainings.

**5.1.5 Informing Communities and receiving complaints**

Each Malaria Consortium office location or project should inform communities on the conduct to expect of staff and partners of the Malaria Consortium. Considerations should be made as to how community members, including children, can raise concerns over inappropriate behaviour by staff. This could include comment boxes, regular announcements to communities in verbal, or written form, ensuring that this is translated into all relevant languages and available in illustrative, low-literacy and/or a child-friendly format where possible.

**5.1.6 Regulation of Communications – Use of Images and information on Children and Adults in Vulnerable Circumstances**

Malaria Consortium recognizes that children and adults in vulnerable circumstances can be unintentionally put at risk through images, video, or other documentation and images. All project managers and partners are responsible for reviewing photography and film captured during the course of their work, before they are used in the public domain, for any potential breach of the Safeguarding Policy.

**Social media**

Malaria Consortium recognizes that there are certain risks particular to children and adults in vulnerable circumstances, which can be posed by staff using work photos on their personal social media sites. For this reason, no staff member, partner, volunteer, trustee, agency, company or consultant employed by Malaria Consortium will post photos relating to the organisation’s activities, on personal social media sites such as Facebook, Twitter, Instagram, without the express permission of the person whose photo has been taken.

**5.2 Responsibilities**

**5.2.1 Staff and Partners**

Part of safeguarding children and adults in vulnerable circumstances is ensuring that all Malaria Consortium staff and partners understand clearly the behaviour that is expected of them when they come into contact with children and adults in vulnerable circumstances.

As well as adhering to the organisations Code of Conduct, all staff and partners are expected to work within the standards outlined below. These Standards are intended to serve as an illustrative guide for staff and partners to make ethical decisions in their professional lives, and at times in their private lives. While acknowledging that local laws and customs may differ from one country to another, these measures are based on international standards:

• Treat all children & adults in vulnerable circumstances (and all beneficiaries) fairly and with respect & integrity and to be aware of the power that they can have over beneficiaries by virtue of their engagement with Malaria Consortium.

• Act in a way that seeks to care for and protect the rights of children & adults in vulnerable circumstances and ensure that their best interests are paramount.

• Safeguard and make responsible use of information and resources. This includes the exercise of due care in all matters of official business, and not divulging confidential information about beneficiaries.

• Uphold the integrity of the organisation, by ensuring that personal and professional conduct is, and is seen to be, of the highest standard.

• Report any abuse by a staff member or partner (regardless of their role) to the relevant Director or Human Resources, and other appropriate authorities.

• Ensure that another appropriate adult is present when working in the proximity of children or adults in vulnerable circumstances.

• Never engage in any exploitative relationships – sexual, emotional, financial or employment-related – with a beneficiary. This is regardless of the local age of consent, i.e., the local or national laws of the country. Failure to report such a relationship may also lead to disciplinary action.

• Refrain from any involvement in criminal or unethical activities that contravene human rights.

• Follow the guidelines when photographing or filming a child or adults in vulnerable circumstances.

• Never shortcut safe recruitment procedures

**5.3 Reporting**

**5.3.1 Incident Reporting**

It is mandatory for any allegation, belief about or suspicion of, abuse, neglect or exploitation of a child or adult in vulnerable circumstances by a Malaria Consortium staff member or partner to be reported immediately to either the respective in-country **Safeguarding Focal Point,** the **Country Director,** the **HR Director** or the **Chief Executive** in the absence of the **HR Director**. Suppliers should report an incident immediately to the relevant national authority. This should be done, **ideally within 24 hours** of the occurrence of the incident or report of the incident.

If a beneficiary (including a child or adult in vulnerable circumstances) or their carer reports an incident, they must be taken seriously and listened to carefully. Once an allegation is made there should be an immediate response that protects them from further potential abuse or victimisation. Where appropriate, the family/carers of the survivor should be informed of the allegation and action proposed and they should be consulted where possible as to the process to be followed.

Beneficiaries should report their concern to a representative of the organisation.

**5.3.2 Confidentiality of reporting**

Reported breaches to the Safeguarding Policy will be kept confidential, and information shared only with relevant individuals. For internal cases, the following parties are likely to be informed: the HR Director, Internal Audit Manager, Chief Executive, and the Board of Trustees. Donors will be informed where there is a mandate to do so and, Trustees will report serious incidents to the Charity Commission. The name of the reporting staff member will be protected, the name of the child or adult

in vulnerable circumstances, their family, and community involved will be kept strictly confidential, and divulged only when absolutely necessary, and then only to relevant individuals.

**5.3.3 External incidents**

There may be cases when Malaria Consortium staff, volunteers and others come across incidents of abuse or exploitation which may be committed by someone not connected with Malaria Consortium, at times within beneficiary communities and at other times in the broader community. Such incidents do not constitute a breach of the Safeguarding Policy, as they have not been perpetrated by a Malaria Consortium staff member or other person or entity associated with Malaria Consortium. However, as children and adults in vulnerable circumstances are beneficiaries in the communities in which Malaria Consortium works, and the health and wellbeing is of paramount concern, staff members have a moral obligation not to ignore external cases, but report to the Country Director and/or the relevant national authority.

**5.4 Breaches**

Any reported breaches of the Safeguarding policy will be ultimately reported to the Chief Executive who will then inform the Board of Trustees.

**5.4.1 Investigation**

Any alleged breach of the Safeguarding policy will be investigated and dealt with.

Investigations will differ depending on the type and severity of the concern, but at a minimum will:

• Have one person who will receive and follow up on concerns and support the investigation.

• Ensure that the Country or Regional Director / HR Director receives the report within 24 hours of the incident occurring or being raised.

• Maintain at all times confidentiality of the alleged offender, the whistle blower, the child or adult in vulnerable circumstances, their family and community.

• Cooperate with local and international authorities, including but not limited to, police in any criminal investigation, keeping in mind the best interests of the child or adult in vulnerable circumstances and their family.

**5.4.2 Disciplinary measures**

Where an investigation involving a member of staff finds there is a case to answer, the employee will be invited to a disciplinary hearing. If upheld, the disciplinary sanction will vary with the severity of the breach and will always be applied using the best interests of the child or adult in vulnerable circumstances. If the disciplinary hearing finds gross misconduct has taken place, the staff member’s contract will be immediately terminated. For less severe breaches, Malaria Consortium will employ various responses ranging from verbal warning, written warning, refresher training and referral to counselling, or a review of current job responsibilities.

**5.4.3 Procedures for criminal breaches**

If it is suspected that the breach is criminal in nature, local authorities will be contacted, taking into account what is in the best interests of the child or adult in vulnerable circumstances and the safety of their family and community. The member of staff or partner will be suspended or removed from contact with children or adults in vulnerable circumstances.

Where it is required by a donor, they should be informed of criminal breaches within the time-frame specified.

**5.5 Support for survivors**

Malaria Consortium will proactively support any staff, partners or beneficiaries who have been victimised during direct interactions with the organisation. Proof of victimisation will not be a pre-requisite for Malaria Consortium to act on a claim. We will work with specialists to identify and make available relevant support that the survivor can then choose to access.

Safeguarding and HR Focal points in our country locations will keep a register of all Suppliers e.g. local charities and government organisations that provide specialist advice, survivor support and counselling. In the event that a member of staff or community member has been victimised and is in need of, or requesting support, Malaria Consortium will work in partnership with these Suppliers. To facilitate access for the survivor to the relevant services the case handler will raise the issue of support. In the case where the trauma may be severe, we will work with specialist organisations to triage and manage the care required.

Malaria Consortium also subscribes to an Employee Assistance Programme that provides first level support locally to any staff member that is in need of counselling and support.

**5.6 Monitoring and Review**

Data and indicators related to implementation of this policy and procedure will be reviewed by the GMG on a quarterly and annual basis. If political, security, or programme changes warrant a more frequent review, it is the responsibility of the Country Director to do so, with support from HQ.

Implementation will also be monitored through regular field project visits. Monitoring of risks to children and adults in vulnerable circumstances, risk mitigation, and the effectiveness of safeguarding measures will be incorporated in the existing Malaria Consortium Quarterly Country Risk Register. This Safeguarding Policy will be reviewed every two years, unless changes in programme, political or security situation warrant earlier action.



**Malaria Consortium Data Protection Policy**



Issued: April 2021

Author: Data Protection Officer Review date: April 2023

Contents

1. [Purpose and context 3](#_bookmark0)
2. [Principles 3](#_bookmark1)
3. [Scope 3](#_bookmark2)
4. [Definitions and terms 4](#_bookmark3)
5. [Implementation 4](#_bookmark4)
	1. [Data Registration 4](#_bookmark5)
	2. [Lawful, fair and transparent data processing 5](#_bookmark6)
	3. [Consent and other conditions for processing data 5](#_bookmark7)
	4. [Implied consent 6](#_bookmark8)
	5. [Explicit consent 6](#_bookmark9)
	6. [The legitimate interest as a condition for processing data 6](#_bookmark10)
	7. [Parental consent 7](#_bookmark11)
	8. [Date processed for specified, explicit and legitimate purposes 7](#_bookmark12)
	9. [Adequate, relevant and limited data processing 7](#_bookmark13)
	10. [Accuracy of data and keeping data up to date 7](#_bookmark14)
	11. [Timely processing 7](#_bookmark15)
	12. [Secure processing 7](#_bookmark16)
	13. [Accountability 7](#_bookmark17)
	14. [Privacy Impact Assessments (PIA) 8](#_bookmark18)
	15. [The rights of data subjects 8](#_bookmark19)
	16. [Keeping data subjects informed 8](#_bookmark20)
	17. [Data subject access 9](#_bookmark21)
	18. [Rectification of personal data 9](#_bookmark22)
	19. [Erasure of Personal Data 10](#_bookmark23)
	20. [Restriction of Personal Data Processing 10](#_bookmark24)
	21. [Data Portability 10](#_bookmark25)
	22. [Objections to Personal Data Processing 11](#_bookmark26)
	23. [Automated Decision-Making 11](#_bookmark27)
	24. [Profiling 11](#_bookmark28)
	25. [Personal Data 11](#_bookmark29)
	26. [Data Protection Measures 12](#_bookmark30)
	27. [Organisational Measures 13](#_bookmark31)
	28. [Data Breach Notification 13](#_bookmark32)

[Appendix A: Data Protection Laws 15](#_bookmark33)

[Appendix B: Data Inventory Schedule 15](#_bookmark34)

[Appendix C: Data Retention Table 15](#_bookmark35)

[Appendix D: Privacy Impact Assessments 16](#_bookmark36)

[Appendix E: Types of privacy risk 16](#_bookmark37)

[Appendix F: Subject Access Request policy and procedure 18](#_bookmark38)

[Appendix G – Data Processor Processing Agreement 20](#_bookmark39)

* + 1. **Purpose and context**

This policy sets out the obligations of Malaria Consortium regarding data protection and the rights of data subjects in respect of their personal data under the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and the Privacy and Electronic Communications Regulation (PECR). Malaria Consortium also has an obligation to uphold the data protection laws in each of the countries it works. A list of relevant laws can be found in Appendix A.

* + 1. **Principles**

Malaria Consortium is committed not only to the details of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

This policy aims to ensure compliance with the GDPR that sets out the following principles in handling personal data. All personal data must be:

1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject;
2. Collected for specified, explicit, and legitimate purposes and not processed or used in a manner that is different with those specified purposes. The exception remains for further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is collected, stored and processed;
4. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or updated without delay;
5. Kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods if it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required under the GDPR in order to safeguard the rights and freedoms of the data subject;
6. Processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
	* 1. **Scope**

This policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must always be followed by Malaria Consortium’s employees, agents, trustees, contractors, subcontractors, interns, volunteers or other parties.

Breaches of the Data Protection Policy shall be dealt with according to Malaria Consortium’s Disciplinary Policy. If there is a possibility that the breach could amount to a criminal offence, the matter shall be referred to the relevant authorities.

All third parties working with or for Malaria Consortium who have or may have access to personal data are required to read, understand and fully comply with this policy. All third parties are required to enter into a data confidentiality agreement prior to accessing any personal data belonging to Malaria Consortium. Malaria Consortium shall always have the right to audit any personal data accessed by third parties.

* + 1. **Definitions and terms**

**Child** means anyone under the age of 18. It may only be lawful to process the personal data of a child under the age of 18 upon receipt of consent from the child’s parent or legal custodian. However, Malaria Consortium regardless of this endeavour, will ensure the rights of the child are upheld.

**Data controller** may be a natural or legal person, whether a public authority, agency or other body which, individually or jointly with others, oversees the purposes and means by which personal data is processed.

**Data subjects** includes current, previous and prospective staff (including employees, interns and volunteers), current, previous and prospective beneficiaries, past and current supporters (donors and funders), trustees, customers and suppliers who can be identified, directly or indirectly, by reference to an identifier such as a name, ID, address, an online identifier or other factors such as physical, physiological, genetic, mental, economic, or social.

**Data subject consent** refers to any specific indication by the data subject that signifies consent to the processing of personal data. Consent may take place by way of a written or oral statement or by clear, unambiguous action and must be given freely at all times, without duress, with the data subject being properly informed.

**Personal data** is any information relating to a data subject.

**Special categories of personal data** refers to data covering racial or ethnic origin, beliefs, whether religious, political or philosophical, membership of a trade-union and data relating to genetics, biometric identification, health, sexual orientation and sex life.

**Third party** is a natural or legal person other than the data subject who is authorised to process personal data, whether a public authority, agency or other body controller, processor or any other person(s) under the direct authority of the controller or processor.

* + 1. **Implementation**
	1. **Data Registration**

Malaria Consortium has registered with the Information Commissioner’s Office (ICO) as a data controller that engages in processing personal information of data subjects. Malaria Consortium will identify all the personal data that it processes and record it in its Data Mapping Inventory Schedule (Appendix B) for each country.

The Data Protection Officer (DPO) will retain a copy of all notifications made by Malaria Consortium to the ICO. The ICO notification schedule is the record of all notifications made.

The ICO notification will be reviewed on an annual basis in April by the DPO, keeping in mind any changes to Malaria Consortium’s activities. These changes will be ascertained by reviewing the Data Inventory Schedule (Appendix B) and by a management review. Privacy impact assessments (Appendix

D) shall be used to ascertain any additional relevant requirements.

* 1. **Lawful, fair and transparent data processing**

GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. GDPR states that processing of personal data shall be lawful if at least one of the following applies:

* The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
* Processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract;
* Processing is necessary for compliance with a legal obligation to which the data controller is subject;
* Processing is necessary to protect the vital interests of the data subject or of other person;
* Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
* Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, where the data subject is a child.
	1. **Consent and other conditions for processing data.**

Consent to the processing of personal data by the data subject must be:

* Freely given and never be given under duress, when the data subject is in an unfit state of mind or provided based on misleading or false information;
* Explicit;
* Specific;
* A clear and unambiguous indication of the wishes of the data subject;
* Informed;
* Provided either in a statement or by unambiguous affirmative action;
* Demonstrated by active communication between the data controller and the data subject and must never be inferred or implied by omission or a lack of response to communication;
* In relation to sensitive data, consent may only be provided in writing, unless there is an alternative legitimate basis for the processing of personal data.

Malaria Consortium will obtain consent to process personal and sensitive data (special categories) when a new data subject signs a contract, consent form or during the induction programmes if they are an employee. Data subjects have the right to withdraw consent at any time.

Malaria Consortium collects information based on legitimate interest when attendees of events, supporters and visitors use its website or give their information to Malaria Consortium staff. The

Privacy Notice on the website clearly explains the reason and purpose for collecting the data, the legitimate interest of the organisation, the name of the data controller, the name of the DPO, details of its data retention policy, information about international data transfers, ways to withdraw consent and details of how to complain about Malaria Consortium to the ICO. ‘Consent’, ‘Legitimate Interest’ or ‘Necessary for Contract’ as a condition are always specified as the reason the data will be processed.

* 1. **Implied consent**

In accordance with the GDPR and with the PECR, implied consent is received when a customer or attendee at an event completes a form or gives their contact details including their email address to the organisation. Malaria Consortium does not use implied consent to promote the aims and objectives of the organisation, merely to deal with contractual arrangements or to answer a request for information about services it provides. Third parties may need to share other people’s data with the organisation, for example, the names of attendees for event or their team/department member details for a research grant approval. This is justified as data protection standards applies to all information shared with the organisation for the performance of a commercial contract. Data must not be kept for no longer than is necessary.

The External Relations team understand that implied consent is for the time being and always ensure the customer, or attendee know that they can Opt-out of future communications whenever they wish by providing an active and working unsubscribe button on the website.

* 1. **Explicit consent**

Explicit consent is used for carrying out tests and research on individuals. The consent forms are kept in line with the research documents retention period.

* 1. **The legitimate interest as a condition for processing data**

Malaria Consortium’s mission is its legitimate interest for processing data as a condition to process the data of supporters and others where risks were assessed and where it may benefit Malaria Consortium as a whole.

When legitimate interest is applied as a condition for processing data the organisation considers the potential impact on any data subjects they may communicate with. The three-stage process to test this is:

* Whether the data subject might reasonably expect their data to be processed. For example, if a previous communication was sent to the data subject, then in many cases they would expect us to process their data unless they told us not to in the past. This assumes that they did not opt-out of future communications, or object to business development efforts.
* Whether legitimate interest might impact adversely on the data subject. For example, if a data subject was a vulnerable person or in a vulnerable circumstance, their data would not be processed. There must be a procedure for ensuring data subjects such as these are suppressed on the data base or ‘forgotten’ if necessary.
* Consider whether any safeguards should be in place to protect data subjects against harm when their data is processed.
	1. **Parental consent**

Parental or custodial consent may be required if/when carrying out research and tests on children, defined as being under the age of 18.

* 1. **Date processed for specified, explicit and legitimate purposes**

Malaria Consortium collects and processes the personal data set out in section 5.25 and for the purposes set out in section 5.2. This may include personal data received directly from data subjects and data received from third parties. The purposes for which personal data will be used will be informed to data subjects at the time that their personal data is collected, by directing them to the Privacy Policy and Cookies Policy on the website, where it is collected directly from them, or within one calendar month after collection where it is obtained from a third party.

* 1. **Adequate, relevant and limited data processing**

Malaria Consortium will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as section 5.6 above.

* 1. **Accuracy of data and keeping data up to date**

All personal data collected and processed must be kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out- of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

* 1. **Timely processing**

Personal data shall not be kept for any longer than is necessary considering the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

* 1. **Secure processing**

All personal data collected and processed must be kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in sections 5.26 and 5.27 of this policy and in the IT User policy on the intranet.

* 1. **Accountability**

Malaria Consortium’s Data Protection Officer (DPO) is Lydia Martin. The DPO reports quarterly to the Governance Committee and Data Protection Board Representative.

Malaria Consortium shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

* The name and details of the DPO, and any applicable third-party data controllers;
* The purposes for which the organisation processes personal data;
* Details of the categories of personal data collected, held, and processed; and the categories of data subject to which that personal data relates (Appendix B: Data Inventory Schedule);
* Details (and categories) of any third parties that will receive personal data from the organisation;
* Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
* Details of how long personal data will be retained by the organisation (Appendix C: Data Retention table)
* Detailed descriptions of all technical and organisational measures taken to ensure the security of personal data.
	1. **Privacy Impact Assessments (PIA)**

A PIA is a process to identify privacy risks and ensure lawful practice when a new project is designed or changes are made to an existing service. Privacy Impact Assessments, when required under the GDPR, shall be overseen by the DPO and will address the following areas of importance:

* The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;
* Details of the legitimate interests being pursued;
* An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
* An assessment of the risks posed to individual data subjects; and
* Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, enough to demonstrate compliance with GDPR.

Appendix D: The PIA template provides more information and the procedure to be followed and Appendix E an Overview of Types of Privacy Risk.

* 1. **The rights of data subjects**

The GDPR sets out the following rights applicable to data subjects:

* + - The right to be informed;
		- The right of access;
		- The right to rectification;
		- The right to erasure (also known as the ‘right to be forgotten’);
		- The right to restrict processing;
		- The right to data portability;
		- The right to object;
		- Rights with respect to automated decision-making and profiling.
	1. **Keeping data subjects informed**

Malaria Consortium shall ensure that the following information is provided, by reference to its Privacy Policy, to every data subject when personal data is collected:

* + - Details of the organisation including, but not limited to, the identity of its DPO;
		- The purpose(s) for which the personal data is being collected and will be processed (as detailed in Section 5.25 of this policy) and the legal basis justifying that collection and processing;
		- Where applicable, the legitimate interests on which the organisation is justifying its collection and processing of the personal data;
		- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
		- Where the personal data is to be transferred to one or more third parties, details of those parties;
		- Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (EEA), details of that transfer, including but not limited to the safeguards in place (see section 5.27 of this policy for further details concerning such third country data transfers);
		- Details of the length of time the personal data will be held (or, where there is no predetermined period, details of how that length of time will be determined (see Appendix C);
		- Details of the data subject’s rights under the GDPR;
		- Details of the data subject’s right to withdraw their consent to processing of their personal data at any time;
		- Details of the data subject’s right to complain to the ICO;
		- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;
		- Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.
		- The information set out above in section 5.13 shall be provided to the data subject at the following applicable time:
			* Where the personal data is obtained from the data subject directly, at the time of collection (links to the Privacy Policy on the website is available in the footer of all outbound communications from Malaria Consortium servers);
			* Where the personal data is not obtained from the data subject directly (i.e. from another party- Joint Controller Agreements are in place with third parties):
				+ If the personal data is used to communicate with the data subject, at the time of the first communication; or
				+ If the personal data is to be disclosed to another party, before the personal data is disclosed; or
				+ In any event, not more than one month after the time at which the personal data is obtained.
	1. **Data subject access**

A data subject may make a subject access request (SAR) to find out more about the personal data which is held about them. The normal respond to SARs is within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension). Please see Appendix E for the Subject Access Request policy and procedures. All subject access requests received must be forwarded to the DPO.

No fee is charged for the handling of normal SARs. Fees will be charged for additional copies of information that is already supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

* 1. **Rectification of personal data**

When the data subject informs that personal data is inaccurate or incomplete, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt of notification from the data subject. (This can be extended by up to two months in the case of complex requests, and in such cases the data subject will be informed of the need for the extension).

If any affected personal data was disclosed to third parties, those parties are to be informed of the rectification to that personal data.

* 1. **Erasure of Personal Data**

Data subjects may request that personal data is erased in the following circumstances:

* + - It is no longer necessary to hold that personal data with respect to the purpose for which it was originally collected or processed;
		- The data subject wishes to withdraw their consent to hold and process their personal data;
		- The data subject objects to the holding and processing their personal data and there is no overriding legitimate interest to allow Malaria Consortium to continue doing so. (See section 5.8 of this policy for further details);
		- The personal data has been processed unlawfully;
		- The personal data needs to be erased to comply with a legal obligation
			* Unless there are reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject’s request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).
			* If any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure, unless it is impossible or would require disproportionate effort to do so.
	1. **Restriction of Personal Data Processing**

Data subjects may request to cease processing the personal data held. If a data subject makes such a request, then only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place can be retained.

If any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

* 1. **Data Portability**

Where data subjects have given their consent to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between Malaria Consortium and the data subject, data subjects have the legal right under the GDPR to receive a copy of their personal data and to use it for other purposes, namely transmitting it to other data controllers, e.g. other organisations.

To facilitate the right of data portability, all applicable personal data to data subjects is to be made available in the following formats:

* CSV files;
* PDF files

Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller. All requests for copies of personal data shall be complied with within one month of the data subject’s request.

* 1. **Objections to Personal Data Processing**

Data subjects have the right to object to the processing of their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

Where a data subject objects to processing their personal data based on its legitimate interests, Malaria Consortium shall cease such processing forthwith, unless it can be demonstrated that legitimate grounds for such processing override the data subject’s interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

Where a data subject objects to processing their personal data for direct marketing purposes, Malaria Consortium shall cease such processing forthwith.

Where a data subject objects to processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under GDPR, ‘demonstrate grounds relating to his or her particular situation’. Malaria Consortium is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

* 1. **Automated Decision-Making**

If personal data is used for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge such decisions under GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from Malaria Consortium.

The right described above does not apply in the following circumstances:

* The decision is necessary for the entry into, or performance of, a contract between Malaria Consortium and the data subject;
* The decision is authorised by law; or
* The data subject has given their explicit consent.
	1. **Profiling**

Where personal data is used or profiling purposes, the following shall apply:

* Clear information explaining the profiling will be provided, including its significance and the likely consequences;
* Appropriate mathematical or statistical procedures will be used;
* Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and
* All personal data processed for profiling purposes shall be secured to prevent discriminatory effects arising out of profiling (see section 5.26 and 5.27 of this Policy for more details on data security and the IT User Policy).
	1. **Personal Data**

The following personal data may be collected, held, and processed:

* + First name, second name, date of birth, gender, ethnicity, phone number, e-mail address, home address, photographs, parental consent, parents’/guardian’s contact details, special needs report such as health and disability for children and adults on the research programmes;
	+ First name, second name, CV, marital status, passport copy, immigration status, National Insurance number, P45/P46/P60 forms, professional/educational records, references, medical records such as disability, home address, phone number, e-mail address, next of kin and protected characteristics from prospective/current staff members including employees, interns and volunteers and bank details of current staff;
	+ First name, second name, company address, company phone number, bank details for invoices to contractors, suppliers and agents;
	+ First name, second name, e-mail address, home address, phone number and bank details of current/previous donors/fundraisers/supporters; and
	+ First name, second name, job title (position), company address, company e-mail address, CV, and company phone number of corporate contacts including contact persons who could lead to major donor or corporate donor relationships.
	1. **Data Protection Measures**

Malaria Consortium shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data, which includes all the additional requirements as per the IT User Policy.

* + - Where emails are sent containing personal data steps should be taken to protect and encrypt.
		- Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded.
		- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.
		- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.
		- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.
		- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail recorded delivery or an equivalent recorded delivery postal service.
		- No personal data may be shared informally and if an employee, intern, volunteer, agent, subcontractor, or other party working on behalf of Malaria Consortium requires access to any personal data that they do not already have access to; such access should be formally requested from the Data Controller/Owner.
		- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar.
		- No personal data may be transferred to any employees, interns, volunteers, agents, contractors, or other parties, whether such parties are working on behalf of Malaria Consortium or not, without the authorisation of the Data Controller/Owner.
		- Personal data must always be handled with care and should not be left unattended or on view.
		- Where personal data is used for Marketing and External Relations purposes, it shall be the responsibility of the Head of External Relations to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and

other platforms such as Social Media accounts and SMS. Such details should be checked at least annually.

* 1. **Organisational Measures**

The following measures must be taken with respect to the collection, holding, and processing of personal data:

All Trustees, employees, interns, volunteers, agents, contractors, or other parties working on behalf of Malaria Consortium shall be made fully aware of both their individual responsibilities and Malaria Consortium’s responsibilities under the GDPR and this policy, and shall be provided with a copy of this policy.

Only employees, interns, volunteers, agents, sub-contractors, or other parties working on behalf of the organisation that need access to, and use of, personal data to carry out their assigned duties correctly shall have access to personal data held by Malaria Consortium.

All employees, interns, volunteers, agents, contractors, or other parties working on behalf of the organisation handling personal data will be appropriately trained to do so.

All employees, interns, volunteers, agents, contractors, or other parties working on behalf of Malaria Consortium handling personal data will be appropriately supervised.

Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.

The performance of those employees, interns, volunteers, agents, contractors, or other parties working on behalf of Malaria Consortium handling personal data shall be regularly evaluated and reviewed.

All employees, interns, volunteers, agents, contractors, or other parties working on behalf of Malaria Consortium handling personal data will be bound to do so in accordance with the principles of the GDPR and this policy by contract.

All agents, contractors, or other parties working on behalf of Malaria Consortium (‘Data Processors’) or work jointly with Malaria Consortium (‘Joint Controllers’) handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Malaria Consortium arising out of this policy and the GDPR.

See Appendix G for a copy of the Data Processor Agreement Template.

Where any agent, contractor or other party working on behalf of Malaria Consortium handling personal data fails in their obligations under this policy that party shall indemnify and hold harmless Malaria Consortium against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

* 1. **Data Breach Notification**

All personal data breaches must be reported immediately to the DPO.

If a personal data breach occurs and that breach is likely to result in a risk to:

* + - the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the DPO must ensure that the ICO is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

If a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the DPO must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

* + - The categories and approximate number of data subjects concerned;
		- The categories and approximate number of personal data records concerned;
		- The name and contact details of the DPO (or another contact point where more information can be obtained);
		- The likely consequences of the breach;
		- Details of the measures taken, or proposed to be taken, to address the breach including, where appropriate, measures to mitigate its possible adverse effects. An incident report form needs to be completed for each breach and the DPO will add to the data incident tracker regardless of whether it is reported to the ICO or not.

******Appendix A: Data Protection Laws**

|  |  |
| --- | --- |
| **Country** | **Data Protection Law** |
| Burkina Faso | Law N°010- 2004/AN |
| Cambodia | Still being developed |
| Chad | LOI 007 Relative a la Protection des Donnees Personnelles |
| Ethiopia | Still being developed |
| Mozambique | African Union Convention on Cyber Security and Personal Data Protection |
| Myanmar | Telecommunications Law and Electronic Transactions Law |
| Nigeria | Nigeria Data Protection Regulation (NDPR) |
| South Sudan | Still being developed |
| Thailand | Personal Data Protection Act of Thailand |
| Togo | Law No. 2019-014 |
| Uganda | The Data Protection and Privacy Act, 2019 |
| United Kingdom | The General Data Protection Regulation |

**Appendix B: Data Inventory Schedule**



Appendix A Data Inventory Schedule.

**Appendix C: Data Retention Table**

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| Data Protection Officer | To ensure that the collection, retention and destruction of all personal data by Malaria Consortium is carried out according to the requirements of the GDPR, PECR and the Data Protection Act 2018. |

|  |  |
| --- | --- |
| Finance Director | To ensure that all financial records, including accounting and tax records are retained for no longer than seven years.To ensure that all relevant statutory and regulatory records are retained for statutory limitation periods (except for the records listed above). |
| Human Resources Director | To ensure that all HR records are retained no longer than six years in total. Unsuccessful applicants’ data must be deleted after six months. All the HR related data must be kept in line with regional legislations. |
| Global Operations Manager | To ensure that all Health and Safety records are retained in accordance with Malaria Consortium’s Public Liability Insurance policy (normally 40 years). |
| Head of External Relations | To ensure that consents are refreshed every two years.To ensure that lapsed contacts data are deleted and/or removed from communications channels. |
| Technical Director | To ensure that children data is kept in line with safeguarding legislations. |

**Appendix D: Privacy Impact Assessments**



Appendix D of the Data Protection Poli

**Appendix E: Types of privacy risk**

**Risks to individuals**

* + - Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
		- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people’s knowledge.
		- New surveillance methods may be an unjustified intrusion on their privacy.
		- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
		- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
		- Identifiers might be collected and linked which prevent people from using a service anonymously.
		- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
		- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
		- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
		- If a retention period is not established information might be used for longer than necessary.

**Compliance risk**

* + - Non-compliance with the common law duty of confidentiality
		- Non-compliance with the DPA.
		- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
		- Non-compliance with sector specific legislation or standards.
		- Non-compliance with human rights legislation.

**Associated organisation/corporate risk**

* + - Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
		- Problems which are only identified after the project has launched are more likely to require expensive fixes.
		- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
		- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
		- Public distrust about how information is used can damage an organisation’s reputation and lead to loss of business.
		- Data losses which damage individuals could lead to claims for compensation.

**Appendix F: Subject Access Request policy and procedure**

This procedure covers all personal data that is processed by Malaria Consortium except for personal data that is routinely requested by data subjects, such as records of staff payslips.

It is the right of all data subjects to ask the following:

1. What personal data at Malaria Consortium is processed about that person, if any;
2. To be provided with a description of the personal data processed by Malaria Consortium about that person;
3. The purpose or purposes for which the personal data is being processed;
4. Confirmation of who will have access to the personal data; and
5. To be provided with a copy of the personal data, as well as a confirmation of where Malaria Consortium acquired that personal data (data collection).
6. **Responsibilities**

The DPO, shall be responsible for the application and functionality of this procedure and shall handle all Subject Access Requests (“SARs”).

The Data Owner/Controller is responsible for the following:

* 1. Keeping a record of all SARs made, including the date on which the SAR was received;
	2. Reviewing all the documents provided to a data subject pursuant to a SAR to check for the mention of any third parties and if a third party is mentioned, to prevent the disclosure of the identity of the third party to the data subject, or to seek written consent from the third party as to the disclosure of their identity.
1. **Procedure**

The data subject is required to provide evidence of their identity by way of a current passport or driving license and theirsignature must be cross-referenced with the signature provided on the Subject Access Request form.

The following information is to be provided by the data subject on the Subject Access Request Form:

* the personal data that is being requested,
* whether specific data or all data held, and
* where it is being held.

The DPO will record the date on which the Subject Access Request Form, with the accompanying identification evidence, is submitted.

Within one month of this date the organisation is to provide to the data subject the personal data requested. If the information is failed to be provided within the one month window, this is a breach of

the GDPR and the Data Protection Act 2018. Extensions shall be allowed at the discretion of the DPO and with reasonable grounds.

It is vital that the Subject Access Form is sent to the DPO, straight away, to ensure that the requested data is collected within the one month window.

The DPO will carry out data collection by one of the following steps:

* 1. Refers the case to the specific data owner who is able to identify the data subject and verify their identity;
	2. The DPO asks for a search of the personal data requested;
	3. The search includes all electronic and hard-copy databases including manual files, backup and archived files as well as email folders and archives.

The Data Owner and the DPO shall always have access to a data map and inventory which sets out the location of all stored data.

At no time may personal data ever be altered or destroyed to avoid disclosure.

1. **Personal data exemption categories**

The following data exemption categories apply, meaning that personal data is not to be provided when covered below:

* The prevention and detection of crime;
* Negotiations with the data subject request maker;
* Management forecasts;
* Confidential references provided by previous employers or referees however not references provided by Malaria Consortium;
* Data covered by legal professional privilege;
* Data used for research, statistical or historical reasons.

Personal data provided by Malaria Consortium to a data subject pursuant to a SAR shall be in electronic format, unless the SAR expressly requests otherwise, and all items shall be scheduled, displaying the data subject’s name and the date on which the data item was delivered.

**Appendix G – Data Processor Processing Agreement**

AGREEMENT DATED [*insert date*]

BETWEEN: **Malaria Consortium a Company Limited by Guarantee Incorporated in England & Wales Company No. 4785712**; and

(2) [ ], having its registered office at [ ] (the "Processor"). BACKGROUND

1. This Agreement is to ensure there is in place proper arrangements relating to personal data passed from Malaria Consortium to the Processor.
2. This Agreement is compliant with the requirements of Article 28 of the General Data Protection Regulation.
3. The parties wish to record their commitments under this Agreement.

IT IS AGREED AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

In this Agreement:

"Data Protection Laws" means the Data Protection Act 2018;

"Data" means personal data passed under this Agreement, being in particular [*describe personal data being passed*];

“GDPR” means the General Data Protection Regulation;

"Services" means [*describe the services provided by the Processor to Malaria Consortium*].

1. DATA PROCESSING

Malaria Consortium is the data controller for the Data and the Processor is the data processor for the Data. The Data Processor agrees to process the Data only in accordance with Data Protection Laws and on the following conditions:

1. The Processor shall only process the Data (i) on the written instructions from Malaria Consortium (ii) only process the Data for completing the Services and (iii) only process the Data in the UK with no transfer of the Data outside of the UK (Article 28, para 3(a) GDPR);
2. Ensure that all employees and other representatives accessing the Data are (i) aware of the terms of this Agreement and (ii) have received comprehensive training on Data Protection Laws and related good practice, and (iii) are bound by a commitment of confidentiality (Article 28, para 3(b) GDPR);
3. Malaria Consortium and the Processor have agreed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, complying with Article 32 of GDPR, details of those measures are set out under Part A of the Annex to this Agreement (Article 28, para 3(c) GDPR);
4. The Processor shall not involve any third party in the processing of the Data without the consent of Malaria Consortium. Such consent may be withheld without reason. If consent is given a further processing agreement will be required (Article 28, para 3(d) GDPR);
5. Taking into account the nature of the processing, assist Malaria Consortium by appropriate technical and organisational measures, in so far as this is possible, for the fulfilment of Malaria Consortium’s obligation to respond to requests from individuals exercising their rights laid down in Chapter III of GDPR – rights to erasure, rectification, access, restriction, portability, object and right not to be subject to automated decision making and etc. (Article 28, para 3(e) GDPR);
6. Assist Malaria Consortium in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR – security, notification of data breaches, communication of data breaches to individuals, data protection impact assessments and when necessary consultation with the ICO, considering the nature of processing and the information available to the Processor (Article 28, para 3(f) GDPR);
7. At Malaria Consortium’s choice, safely delete or return the Data at any time. [It has been agreed that the Processor will in any event securely delete the Data at the end of the Services]. Where the Processor is to delete the Data, deletion shall include destruction of all existing copies unless otherwise a legal requirement to retain the Data. Where there is a legal requirement the Processor will prior to entering into this Agreement confirm such an obligation in writing to Malaria Consortium. Upon request by EIG Group the Processor shall provide certification of destruction of all Data (Article 28, para 3(g) GDPR);
8. Make immediately available to Malaria Consortium all information necessary to demonstrate compliance with the obligations laid down under this Agreement and allow for and contribute to any audits, inspections or other verification exercises required by Malaria Consortium from time to time (Article 28, para 3(h) GDPR);
9. Arrangements relating to the secure transfer of the Data from Malaria Consortium to the Processor and the safe keeping of the Data by the Processor are detailed under Part A of the Annex.
10. Maintain the integrity of the Data, without alteration, ensuring that the Data can be separated from any other information created; and
11. Immediately contact Malaria Consortium if there is any personal data breach or incident where the Data may have been compromised.
12. Termination

Malaria Consortium may immediately terminate this Agreement on written notice to the Processor. The Processor may not terminate this Agreement without the written consent of Malaria Consortium.

1. General
	1. This Agreement may only be varied with the written consent of both parties.
	2. For the purposes of this Agreement the representatives of each party are detailed under Part B of the Annex.
	3. This Agreement represents the entire understanding of the parties relating to necessary legal protections arising out of their data controller/processor relationship under Data Protection Laws.
	4. This Agreement is subject to English law and the exclusive jurisdiction of the English Courts.

For and on behalf of Malaria Consortium

………………………………………………….

For and on behalf of [ ]

………………………………………………….

**ANNEX**

**Part A**

Compliance with Article 32, para 1 of GDPR

1. Consideration of anonymisation, pseudonymisation and encryption.

*Is the above possible? If not, please explain why. If possible please insert details.*

1. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and related services.

*Please explain how the above will be delivered.*

1. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

*Please confirm the above is possible and description of process in place to deliver the above.*

1. A process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the processing.

*Please confirm the above process is in place and broadly what that process is.*

Compliance with Article 32, para 2 of GDPR

1. In assessing the appropriate level of security account shall be taken of the risks that are presented by processing, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data transmitted, stored or otherwise processed.

*Please describe secure transfer process from Malaria Consortium to the Processor and levels of security to be applied by the Processor when the Data is in their possession.*

Compliance with Article 32, para 3 of GDPR

1. Adherence to an approved code of conduct referred to in Article 40 (GDPR) or an approved certification mechanism as referred to in Article 42 (GDPR) may be used as an element by which to demonstrate compliance with the requirements set out in para 1 of GDPR – see above.

*Please describe any relevant code of practice relied upon.*

Compliance with Article 32, para 4 of GDPR

1. The Processor to ensure that anyone acting on their behalf does not process any of the Data unless following instructions from Malaria Consortium unless they are required to do so under English law.

**ANNEX**

**Part B**

Malaria Consortium Representative shall be [*insert details*] or such other person as shall be notified by Malaria Consortium [*insert details*].

The Processor Representative shall be [*insert details*] or such other person as shall be notified by the Processor [*insert details*].