Data Protection policy and procedures

Information Commissioner Officer's Data Protection Registration No. Z6664020 (CARE International UK) and No. Z8127893 (CI Enterprises)

Controller: CARE International UK

Responsible Person: Shabnam Amini, Executive Director

CARE International UK
89 Albert Embankment
London, SE1 7TP
020 7091 6000

1. Aims of this policy

CARE International UK (**CIUK**) is committed to protecting personal data. For CIUK personal data can be related to relationships we hold with supporters, volunteers and donors, as well as data on job candidates, employees, trustees, suppliers and certain other third parties or beneficiaries of CARE International's poverty fighting work. CIUK need to keep certain information to carry out our day to day work - enabling our mission by fundraising, through campaign actions, monitoring our programme impact and by providing evaluation reports to funders and supporters.

CIUK is committed to ensuring any personal data will be dealt with in line with the EU General Data Protection Regulations ("**GDPR**"). To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy (the "**Policy**") is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection principles and procedures. This document also highlights key data protection procedures within the organisation. Your understanding and compliance with this Policy is key to ensuring we meet our obligations under the GDPR so please read it carefully. If you have any questions when implementing this Policy, please contact the Data Protection Working Group:

London-DataProtection@careinternational.org

2. Definitions

In line with Article 5 of the GDPR, CIUK requires that personal data it processes and collects shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data 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 by the GDPR in order to safeguard the rights and freedoms of individuals and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Please refer to the IT and Network Policy and Procedures for more detail.

Personal data is any data which lets you identify a living individual. Personal data can be factual (for example, a name, business email address, phone number or date of birth) or it can be an opinion about that person, their actions or behaviour. If you can't use a piece of data to identify an individual, but can combine it with other data we hold to identify an individual then all of that data is personal data.

Please be aware that the GDPR defines personal data broadly. Personal data goes beyond obvious details that can identify individuals, such as their name or address. If you are unclear whether the data you are handling is personal data please contact the Compliance Team.

Please note that the GDPR makes a specific distinction between personal data and special categories of personal data. Where CIUK processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the GDPR requirements of special categories of data and criminal records data. If you are processing special categories of personal data, please contact the Data Protection Working Group for appropriate guidance.

A 'Data Subject' is a natural person whose personal data is processed by a controller or processor. Employees, trustees, volunteers, supporters, donors and beneficiaries are examples of Data Subjects whose data may be processed by CIUK.

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper-based personal data as well as that kept electronically. The GDPR defines "processing" broadly, and if you are handling personal data in any way it is likely you will be processing it for the purposes of the GDPR.

Definitions of roles:

- **Controller**: a controller determines the purposes and means of processing personal data.
- **Responsible Person**: an individual within the organisation responsible for ensuring compliance with this Policy who is the point of contact for information requests, as well as reporting any breaches to the Information Commissioner's Office (ICO).

3. Scope of this policy

This Policy applies to our office in the UK and to all people who handle work for the UK or any associated entities including directors, employees and all temporary or contract staff, and volunteers whether or not they are employed by CIUK and irrespective of length of service or duration of contract.

4. Processing personal data lawfully

You must only process personal data where it is necessary and CIUK has a valid lawful basis to do so.

The lawful bases for processing that apply to personal data processed by CIUK are set out below. You must ensure that at least one these bases apply whenever CIUK processes personal data:

(a) **Contract**: the processing is necessary for a contract CIUK has with a data subject, or because a data subject has asked CIUK to undertake specific steps before entering into a contract with CIUK.

(b) **Legal obligation**: the processing is necessary for CIUK to comply with its legal or regulatory obligations e.g. anti-money laundering and terrorist financing.

(c) **Legitimate interests**: the processing is necessary for CIUK's legitimate interests or the legitimate interests of a third party, and CIUK is sure that these interests are not overridden by a data subject's own rights or interests which need protecting. CIUK's legitimate interests are generally:

(i) legal - e.g. filing, enforcing or defending against legal claims or the collection of outstanding debt; or

(ii) commercial - e.g. avoiding breaches of contract, conducting campaign actions, monitoring our programme impact, providing evaluation reports to funders and supporters, for marketing, for research purposes, to administer donations, to contact supporters, volunteers, donors and trustees, to administer our programmes.

(d) **Consent**: Where no other lawful basis set out above is fulfilled, CIUK may process personal data on the basis of the individual's consent. The individual must have freely given clear, informed and unambiguous consent by an affirmative action to CIUK to process their personal data for a specific purpose that has been informed to them. Please note that consent should be avoided in those circumstances where it is not practicable for CIUK to stop processing certain personal data if an individual where to withdraw their consent to it (i.e. in the employment context).

If you intend to use consent or legitimate interests for your intended processing activity or are in any way unsure whether an alternative lawful basis can be applied to your processing of personal data, you must speak to the Data Protection Working Group.

5. Examples of information processed

CIUK processes personal data of the following individuals:

5.1 Candidates and employees

- Data on applicants for posts, including references

- Employee payroll and performance data – contact details, bank account number, payroll data, supervision and appraisal notes are all kept for the duration of employment and 25 years thereafter in paper form
- Ethnic origin, religion and disabilities are held electronically and this data is not shared outside of the Human Resources team
- Employee contact details including email, telephone and family details (e.g. next of kin) are all kept for the duration of employment and 6 years thereafter electronically
- Users – contact details (in many voluntary organisations, detailed case notes may be held)

5.2 Supporters, donors, trustees, volunteers, enquirers and complainants

- Personal data including address, email address and telephone number(s)
- Bank account details for direct debits (where applicable)
- For event participants data including, but not limited to, medical data and emergency contacts

5.3 Beneficiaries

- Data on individuals who participate in programmes including, but not limited to, name, address, family details and date of birth are held electronically
- Consented images of individuals with their corresponding case study are held electronically on www.careimages.org Images can be used publically through online and offline communications channels. Individuals have the right to remove consent at any time.
- Personal data on people who participate in programmes must be held under one of two conditions, either:

  i. By determining that there is a legitimate interest in us keeping the data which is determined through a legitimate interest assessment (LIA); or

  ii. By gaining, and being able to demonstrate, the consent of the person to store that data.

- Data to be kept for periods of up to 5 years, or for as long as necessary in order to fulfil the requirements of the donor or for audit purposes.

6. How data is kept

- Personal data is kept electronically and in paper form.
- Groups of people within the organisation who will process personal data are employed staff and volunteers.
- Data used externally for research purposes will be made anonymous. This can be academia or market research companies who are employed to analyse our performance and ensure we continue to learn and improve our programme and fundraising practices.

7. Third party service providers

CIUK uses third party service providers to process [both employee-related and trustee-related personal data and personal data of donors, supporters, volunteers and beneficiaries.

CIUK requires that all third-party service suppliers with access to personal data of employees, donors, supporters and beneficiaries comply with applicable data protection laws. CIUK ensures that all new third-party service providers undergo appropriate due diligence to assess their understanding of, and compliance with, CIUK's information security and data protection

requirements. All new contracts that include the processing of personal data must be reviewed by the department Director and referred to the Data Protection Working Group.

A record of all third-party data processors is held by the relevant Head of department.

CIUK requires that it has written agreements in place with all its third-party service providers [who are processing personal data on CIUK's behalf] which include appropriate data protection obligations as required by the GDPR that have been approved by the Data Protection Working Group. Such provisions shall include the subject matter and duration of the processing, nature and purpose of the processing, the type of personal data and categories of data subjects and the rights and obligations of CIUK as the controller.

8. Informing the individual – Privacy Notices

CIUK is required by law to provide employees, trustees, volunteers, supporters, beneficiaries and donors with a clear and transparent notice which sets out the way in which CIUK processes their personal data.

All CIUK privacy notices are available in writing and must be in electronic form, for example, on our website. If requested by an individual, notices should be made available orally or in such format which is reasonably accessible to them.

CIUK's Employee Privacy Notice is relevant for all employee-related personal data and is available on the CIUK intranet. CIUK's External Privacy Notices are relevant for all website-users, donors, supporters, trustees and volunteers whose personal data is processed and are accessible below:

http://www.careinternational.org.uk/privacy-policy

https://www.lendwithcare.org/info/terms/privacy

You should make the appropriate privacy notice available to a data subject at the time personal data is collected from them. For example, a privacy notice should be made available to employees by including the information in their employment contract package, and volunteers, donors and supporters should be directed towards the Privacy Notice on the CIUK website when we start processing their data (e.g. when we respond communicate with them the first time).

For new processing activities (i.e. additional purposes to those for which CIUK originally collected the personal data), you must notify the relevant individuals before any personal data is used for the new processing activity.

Where information is collected from an employee, volunteer, donor, supporter, trustee or beneficiary for the same purpose, a privacy notice only needs to be provided once. For example, if an employee provides HR with an update of their qualifications and skills on an annual basis, HR will not provide a privacy notice each time.

9. Records of data processing activities

CIUK, which is required to do so under the GDPR, maintains a formal, written record of its data processing activities, and the relevant data protection authorities can ask CIUK for copies of these at any time. Please contact the Data Protection Working Group if you would like to see copies of these records.

While it is the responsibility of certain nominated data protection persons to ensure that this record is accurate and up to date, before undertaking any processing of personal data please review the

record to check that your intended processing fits within the scope of the record and contact the Data Protection Working Group before processing if you have any doubts.

10. Third party transfers of personal data

10.1 Transfers to third party service providers

Before transferring any personal data to third parties outside of the EEA or to third party service providers whose servers are located outside the EEA, CIUK requires a data processing contract to be entered into with the third party, which details the terms around the transfer and the subsequent processing of personal data.

Where the transfer is to a country outside of the EEA (excluding Adequate Countries (defined below)) CIUK shall also require the EU Commission standard contractual clauses (controller to processor) are included in the above data processing contract.

Adequate Countries includes any country which has received approval from the EU Commission for having implemented data protection laws which adequately protect personal data. Currently these countries are Andorra, Argentina, Canada (for organisations that are subject to Canada's PIPEDA law), Switzerland, the Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, and Uruguay.

We have entered into contracts that include data protection clauses with our third-party service providers who are located outside the EU and process data of EU individuals. Please see section 7 of this Policy for further details on third party service providers.

Any contracts being entered into with third party service providers which relate to the transfer of personal data must be reviewed and approved by the relevant Head of department and/or Executive Director.

11. Responsibilities

Overall responsibility for personal data in a not-for-profit organisation resides with the governing body. In the case of CIUK, this is the Board of Trustees.

The governing body delegates tasks to the Data Protection Working Group at CIUK. The Group is responsible for:

- understanding and communicating obligations under GDPR;
- identifying potential problem areas or risks; and
- producing clear and effective procedures.

All employed staff and volunteers who process personal data must ensure they not only understand, but also act in line with this Policy.

12. Policy implementation

12.1 To meet our responsibilities employees, contractors, suppliers, volunteers and trustees will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of data needed is collected and used;
- Ensure the data used is up to date and accurate;
- Review the length of time data is held;

- Ensure it is kept safely; and
- Ensure the rights people have in relation to their personal data can be exercised.

12.2 The Data Protection Working Group will ensure that:

- Everyone managing and handling personal data is trained to do so;
- All employees of CIUK are trained on the GDPR through online training
- Anyone wanting to make enquiries about handling personal data, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures; and
- Queries about handling personal data will be dealt with swiftly and politely and in accordance with the Information Commissioner's guidelines.

13. Privacy Impact Assessment and Privacy by Design

In order to maintain compliance with data protection requirements it is important that we identify early whether any new systems, processes, services or projects are likely to impact on data protection. When using our standard business case or service tender template, we will consider whether there are any data protection implications "Privacy by design" is the ethos of promoting data protection from the start of a project and, where appropriate, you will need to ensure that a 'Privacy Impact Assessment' ("PIA") will be completed and that the project commences with a privacy plan. If you need further guidance or believe a PIA is required for your project please contact the Data Protection Working Group.

14. Training CIUK employees

At CIUK we have a data protection working group including representatives from IT, Finance, HR, Fundraising and Programmes & Policy. This group is chaired by a member of the Senior Management Team. The group is responsible for:

- internal policies
- training of staff
- awareness raising
- ensuring systems are robust
- identifying and mitigating risks
- carrying out internal audits
- reporting on any breaches

Training and awareness-raising about the GDPR and how it is followed at CIUK takes the following forms:

- On induction: each new employee, volunteer or board member will be introduced to this Policy during their HR induction on the first day of employment/volunteering. An online GDPR training course is also compulsory as part of the induction. In addition a presentation is made by a member of the Data Protection Working Group to all new staff at a quarterly induction.
- General awareness of data protection will be promoted internally through posters placed in key areas e.g. tea stations, meeting rooms, photocopy/print machines.
- All employees, volunteers and board members sign a data protection Policy statement, declaring they understand their responsibility in protecting personal data.
- Refresher training will be provided by the Data Protection Working Group on an annual basis or as and when regulations change.

15. Gathering and checking data

Before personal data is collected, we will consider the GDPR requirements to ensure we adhere. CIUK requires that all processing of personal data (including by its third party service providers) is carried out in a way that ensures the personal data's security and implements CIUK's information security requirements.

We will take the following measures to ensure that personal data kept is accurate and safe:

- Using lockable cupboards with restricted access to keys;
- Setting up computer systems to allow restricted access to database systems;
- Remotely remove CIUK data from mobile phones;
- Back up of data on servers, and we have a disaster recovery plan in place;
- Encrypted attachments for sensitive personal data sent by email.
- Paper-based data is destroyed by a confidential waste supplier (www.shredit.co.uk);
- On-going reviews of security measures; and
- Regular security testing and annually we undertake external penetration testing.
- Our IT Security and Network Policy is available on the CIUK intranet.

Personal data will not be used apart from the exact purpose for which permission was given to process it.

16. Data Breaches

CIUK is under an obligation to report material data breaches to the Data Protection Authority and, in some cases, the individuals whose data has been breached themselves. We must also document each data breach, however small, in an internal breach register.

You must therefore report any actual or potential breaches of personal data to the Data Protection Working Group as soon as you become aware of them. For further information, please see our Data Breach Policy [found on the CIUK intranet].

17. Data Subject Requests

Anyone whose personal data we process has the right to:

- Know what personal data we hold and process on them;
- Gain access to this personal data (commonly known as a "**Subject Access Request**");
- Know how to keep their personal data up to date;
- Ask us to delete personal data we hold about them under certain circumstances (for example, where it is no longer necessary for our purposes);
- Ask us to freeze our processing of their personal data under certain circumstances (for example, where they challenge the accuracy of the data we hold about them); and
- Ask us to correct any inaccurate personal data we hold about them.

Furthermore, if our processing of the Data Subject's data is based on consent the Individual also have the right to withdraw this consent at any time.

Any person wishing to exercise these rights should apply in writing by post or by email to the CIUK Supporter Care team:

CARE International UK, 9th Floor, 89 Albert Embankment, London, SE11 7TP

supportercare@careinternational.org

If you receive a Subject Access Request, the first step is to inform the Data Protection Working Group who will advise you on how to proceed.

If the request is very simple and specific such that you can identify exactly what the person is asking for, and there are no reservations whatsoever about giving out the information which has been requested, then you may be advised to supply the information which is being requested. If so, you must do this without undue delay and at the latest within one month of receiving the request.

If there are any concerns about giving out the information, the Data Protection Working Group may decide to escalate the request, in which case you do not need to do anything further. The type of situations which might cause concern are: (i) if the information requested contains data about a third party; or (ii) if we are in a dispute with the person making the request.

If you receive a request from an individual to exercise any of the other subject rights discussed above, please escalate to the Data Protection Working Group who will provide further information on how to manage and respond to this request.

Before responding to any request from an individual we require proof of identity. The following forms of ID will be required: copy of a passport, driving licence or utilities bill.

Queries about handling personal data will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal data as soon as possible, but will ensure it is provided within one month of receiving the request.

CIUK does not charge individuals to carry out their requests for accessing, correcting, amending, deleting personal data. However, if you receive repetitive requests, requests that are clearly unfounded or excessive or request for multiple copies of information, please contact the Data Protection Working group, as CIUK may be entitled to charge a reasonable fee for them.

18. Reviewing this Policy

This policy will be reviewed every two years to ensure it remains up to date and compliant with the law.

19. Declaration (for internal use only)

I confirm I have read and understood CIUK's Data Protection Policy and will act in accordance with it.

I am connected with this organisation in my capacity as a

☐ Employee

☐ Contractor

☐ Volunteer

☐ Trustee/committee member

Signature:

Print name:

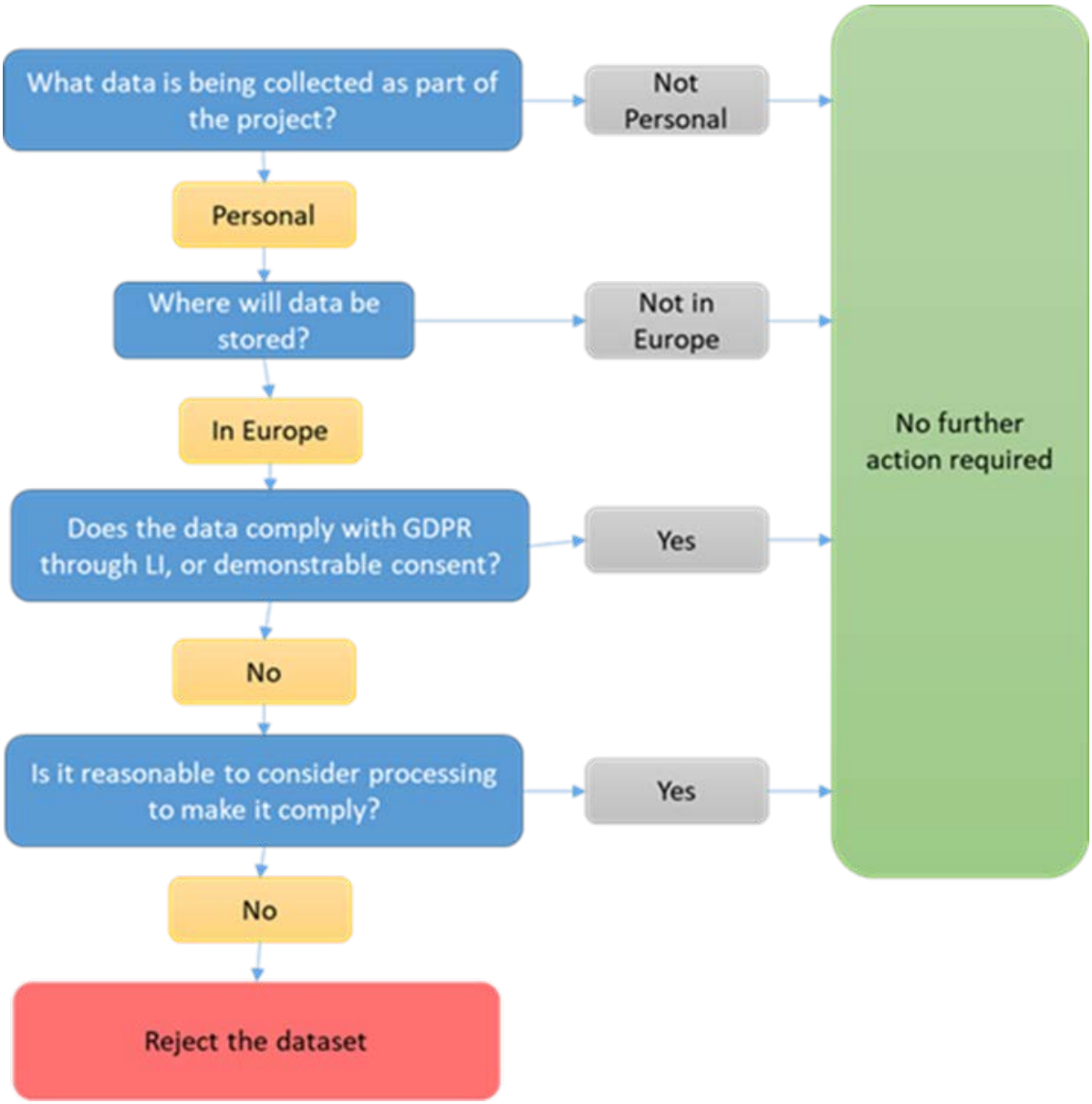
Date:

Please return this form to Jacqueline Salvage, HR Officer, CARE International UK. Jacqueline is a member of CIUK's Data Protection Working Group.

Annex 1

For staff use only

Data protocol for participant data use (added 12 July 2019)



LI = Legitimate Interest. The ICO legitimate interest assessment form must be completed to determine this.