



Data Protection Policy

Ubaka U Rwanda

Last updated	May 2018
--------------	----------

Definitions

Charity	means Ubaka U Rwanda, a registered charity.
GDPR	means the General Data Protection Regulation.
Responsible Person	Lucy White

1. Data protection principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals;
- b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d. 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;
- e. 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



- f. 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.”

2. General provisions

- a. This policy applies to all personal data processed by the Charity.
- b. The Responsible Person shall take responsibility for the Charity’s ongoing compliance with this policy.
- c. This policy shall be reviewed at least annually.
- d. The Charity is exempt from registering at the Information Commissioner’s Office as an organisation that processes personal data given it is a non-for-profit that only process information necessary to establish or maintain membership or support

3. Lawful, fair and transparent processing

- a. To ensure its processing of data is lawful, fair and transparent, the Charity shall only hold a list of supporters names and their email addresses necessary to establish and maintain membership or support. The information will be held on Mail Chimp which is encrypted (for further information see <https://mailchimp.com/about/security/>)
- b. There may be times where physical addresses or phone number may be necessary to be collected and stored. Where this is deemed necessary informed consent shall be obtained, all data will be encrypted and follow all other terms of the privacy policy.
- c. Individuals have the right to access their personal data and any such requests or Subject Access Requests made to the charity shall be dealt with in a timely manner, specifically within 40 calendar days’.

4. Lawful purposes

- a. All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests ([see ICO guidance for more information](#)).
- b. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data. Individuals are only added to the supporter list if they sign up via the website and click an e-mail to confirm they want to join
- c. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent will be clearly available at the bottom of the email and the Responsible Individual will then immediately remove the individual’s details from the Mail Chimp list.
- d. Ubaka U Rwanda is led by a Trustee group that is resident both in inside and outside the EU. Based on this there may be a need to share data outside the EU. This will only be done when it is essential to conducting their fiduciary responsibility and where data is securely transferred (encrypted) and stored in a secure way.



5. Data minimisation

- a. The Charity shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. For this reason only names and emails are held of supporters, no further information is held

6. Accuracy

- a. The Charity shall take reasonable steps to ensure personal data is accurate.
- b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

- a. To ensure that personal data is kept for no longer than necessary, the Charity shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

- a. The Charity shall ensure that personal data is stored securely using modern software that is kept-up-to-date. For this reason encrypted Mail Chimp is used.
- b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- c. When personal data is deleted this should be done safely such that the data is irrecoverable.
- d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Charity shall promptly assess the risk to people's rights and freedoms and will report this breach to the ICO ([more information on the ICO website](#)) with 72 hours of finding out.

END OF POLICY