Data Protection Policy

Namibia Project

Last updated	2nd April 2020

Definitions

Charity	means Namibia Project, a registered charity.
GDPR	means the General Data Protection Regulation.
Responsible Person	means Rijn Brandse.
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Charity.

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 shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

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 appendix 1).
b. The Charity shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

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.
b. [Add considerations relevant to the Charity's particular systems]

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.
c. [Add considerations relevant to the Charity's particular systems]

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.
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 if appropriate report this breach to the ICO (See appendix 2).

END OF POLICY

Appendix 1

The lawful basis for processing

- You must have a valid lawful basis in order to process personal data.
- There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.
- Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.
- You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.
- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
- If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).
- If you are processing special category data, you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- If you are processing criminal conviction data or data about offences, you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

Checklist

□ We have reviewed the purposes of our processing activities and selected the most appropriate lawful basis (or bases) for each activity.

□ We have checked that the processing is necessary for the relevant purpose and are satisfied that there is no other reasonable way to achieve that purpose.

□ We have documented our decision on which lawful basis applies to help us demonstrate compliance.

□ We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.

□ Where we process special category data, we have also identified a condition for

processing special category data and have documented this.

□ Where we process criminal offence data, we have also identified a condition for processing this data and have documented this.

Appendix 2

Personal data breaches

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Checklists

Preparing for a personal data breach

□ We know how to recognise a personal data breach.

□ We understand that a personal data breach isn't only about loss or theft of personal data.

□ We have prepared a response plan for addressing any personal data breaches that occur.

□ We have allocated responsibility for managing breaches to a dedicated person or team.

□ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach

□ We have in place a process to assess the likely risk to individuals as a result of a breach.

□ We know who is the relevant supervisory authority for our processing activities.

□ We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.

□ We know what information we must give the ICO about a breach.

□ We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.

□ We know we must inform affected individuals without undue delay.

□ We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.

□ We document all breaches, even if they don't all need to be reported.