

ZANE: Zimbabwe A National Emergency Data Protection Policy

ZANE: Zimbabwe A National Emergency is committed to processing data in accordance with its responsibilities under the General Data Protection Regulation (GDPR). Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and/or 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;
3. adequate, relevant and/or limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; reasonable steps 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;
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 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
6. processed in a manner that ensures appropriate security of the personal data, including reasonable protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”
 - This policy applies to all personal data processed by ZANE.
 - The Chief Executive shall take responsibility for ZANE’s ongoing compliance with this policy.
 - This policy shall be reviewed at least annually.
 - ZANE is registered with the Information Commissioner’s Office (ICO) as an organisation that processes personal data.

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.

Any person who wishes to exercise this right should make the request in writing to the Chief Executive. ZANE reserves the right to charge a fee for each subject access request. If personal details are inaccurate, they can be amended upon request.

ZANE aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

Lawful purposes

1. 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.
2. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
3. 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 ZANE's systems.
 - ZANE shall ensure that personal data are adequate, relevant and/or limited to what is necessary in relation to the purposes for which they are processed.
 - ZANE shall take reasonable steps to ensure personal data are accurate.
 - Where necessary for the lawful basis on which data are processed, reasonable steps shall be put in place to ensure that personal data are kept up to date.

Archiving / removal

1. ZANE will not keep personal data for any longer than necessary

Security

ZANE shall take reasonable steps to ensure that personal data are stored securely.

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.

When personal data are deleted this should be done safely such that the data is irrecoverable.

Appropriate back-up and disaster recovery solutions shall be in place.

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, ZANE shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

This policy is subject to adherence to any changes in GDPR legislation.

ZANE has a separate **Card Data Policy** reflecting its commitment to comply with required standards governing the security of sensitive and confidential information. The purpose of this security policy is to establish rules to insure the protection of confidential and/or sensitive information stored or transmitted electronically and to ensure protection of ZANE's information technology resources. The policy assigns responsibility and provides guidelines to protect ZANE's systems and data against misuse and/or loss. This security policy applies to all users of computer systems, centrally managed computer systems, or computers that are authorized to connect to ZANE's data network.

Responsibility for ensuring this policy is adhered to rests with the Chief Executive.

Date policy adopted: April 2017

Last Reviewed: December 2019

Due for review: October 2020