PRIVACY POLICY

Data Protection Policy

Definitions
We refers to https://www.the9.cy/
GDPR means the General Data Protection Regulation.
Responsible Organization means **The 9.**
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 9 is committed to processing data following its responsibilities under the GDPR.
Article 5 of the GDPR requires that personal data shall be:
a. processed lawfully, fairly, and transparently concerning 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 concerning 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 inaccurate personal data, 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 the implementation of the appropriate technical and organizational measures required by the GDPR 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 unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures."

2. General provisions

a. This policy applies to all personal data processed by us.
b. The Responsible Person shall take responsibility for the 9's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.

3. Lawful, fair, and transparent processing

a. To ensure its processing of data is lawful, fair, and transparent, we 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 data and any such requests made to us shall be dealt with promptly.

4. Lawful purposes

a. All data processed by the 9 must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task, or legitimate interests.
b. We 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 available and systems should be in place to ensure such revocation is reflected accurately in our systems.

5. Data minimization

a. We shall ensure that personal data are adequate, relevant, and limited to what is necessary concerning the purposes for which they are processed.
b. We shall take reasonable steps to ensure personal data is accurate.
c. 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.

6. Archiving & removal

a. To ensure that personal data is kept no longer than necessary, we 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.

7. Security

a. The 9 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 unauthorized 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.

8. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, we shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach.