



## Privacy policy

### 1. Data protection principles

Cameroon Check is committed to processing data in accordance with EU's GDPR (General Data Protection Regulation) regulations, Cameroon media laws and ethics, journalism canons and in line with this best practice for individuals outside the EU.

Article 5 of the EU's GDPR requires that personal data 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.
- 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.
- 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 EU's GDPR in order to safeguard the rights and freedoms of individuals.
- 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

- All personal data that the organisation processes is covered by these guidelines.
- The responsible person is in charge of ensuring that the organisation abides by these guidelines going forward.
- Every year, these guidelines will be reviewed.

## 3. Lawful, fair and transparent processing

- The organisation is required to keep a Register of Systems in order to guarantee that its data processing is ethical, just, and lawful.
- Every year, the Register of Systems will be reviewed.
- People have the right to access their personal data, and the organisation must respond promptly to any requests made in this regard.

## 4. Lawful purposes

- The following legal basis must be used by the organization for any data processing: permission, contract, legal requirement, vital interests, public task, or legitimate interests <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>
- The organization must record the proper legal justification in the register of systems.
- Evidence of opt-in consent must be stored with the personal data when consent is used as a legal basis for processing it.
- The ability for an individual to revoke their consent should be made explicit if communications are delivered to individuals based on that consent, and processes should be in place to guarantee that such revocation is appropriately registered in the organisation's systems.

## 5. Data minimisation

- The organisation must make sure that personal data is sufficient, pertinent, and kept to a minimum essential for the purposes for which it is handled.
-



- Your email address and any other personal information about you will not be included in the "online identifiers" that the organisation collects through third-party plugins, such as IP addresses.
- Through the use of third-party systems, the organisation will only gather and use personal data as needed to accomplish these goals and where it can depend on one of the legal bases specified in the complete Terms and Conditions. With the user's prior authorization, data will be gathered for the following reasons, including but not limited to:
  - subscriptions to newsletters
  - user comment or input
  - workshops and award nominations
  - Donations
  - Client and donor reporting

## 6. Accuracy

- To guarantee the accuracy of personal data, the organisation must take appropriate measures.
- Steps must be taken to guarantee that personal data is maintained current when they are required by the legal basis for processing the data.
- On request, the organisation will make a reasonable effort to update any information that the user believes to be incorrect, out-of-date, incomplete, irrelevant, or misleading. Email inquiries should be sent to the [info@camerooncheck.cm](mailto:info@camerooncheck.cm)

## 7. Archiving / removal

- The organisation should establish an archiving policy for each area in which personal data is handled and evaluate this policy yearly to ensure that personal data is stored for no longer than required.
- The archiving policy will consider what data should or must be preserved, why, and for how long.

## 8. Security



- The organisation is responsible for making sure that personal data is stored safely and securely using current software.
- Personnel with a need for access should only have access to personal information, and security measures should be in place to prevent unauthorized sharing of data.
- When personal information is erased, it should be done securely so that it cannot be recovered.
- Solutions for disaster recovery and appropriate backup must be in place.

## 9. Breach

The organisation shall promptly assess the risk to people's rights and freedoms in the event of a security breach that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data and, if necessary, report this breach to the relevant authorities.



# CAMEROON *CHECK*

Tel: 659 798 836  
Location: Buea, Cameroon  
[www.camerooncheck.cm](http://www.camerooncheck.cm)

Email: [info@camerooncheck.cm](mailto:info@camerooncheck.cm)