



Data Protection Policy

POLICY NO.

008

Centre de Recherche sur l'Anti-Corruption (CERC)

CERC policies and procedures

Data protection principles



The Centre de Recherche sur l'Anti-Corruption (CERC) is committed to ensuring that personal data are:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. 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 incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. 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;
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 they 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 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 protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

General provisions

1. This policy applies to all personal data processed by CERC.

2. The Monitoring, Evaluation and Learning Officer takes responsibility for CERC's ongoing compliance with this policy.
3. This policy is reviewed at least once a year.

Lawful, fair and transparent processing

1. To ensure that its processing of data is lawful, fair and transparent, CERC maintains a register of systems.
2. The register of systems is reviewed at least once a year.
3. Individuals have the right to access their personal data, and any such request made to CERC will be dealt with in a timely manner.

Lawful purposes

1. All data processed by CERC must be processed on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
2. CERC must record the appropriate lawful basis in the register of systems.
3. Where consent is relied upon as a lawful basis for processing data, evidence of explicit consent must be kept with the personal data.
4. Where communications are sent to individuals on the basis of their consent, the option for the individual to revoke their consent must be clearly available, and systems must be in place to ensure that such revocation is reflected accurately in CERC's systems.

Data minimisation

CERC must ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

1. CERC takes reasonable steps to ensure that personal data are accurate.

Accuracy (continued)

2. Where necessary for the lawful basis on which data are processed, steps are put in place to ensure that personal data are kept up to date.

Archiving and removal

1. To ensure that personal data are kept for no longer than necessary, CERC puts in place an archiving policy for each area in which personal data are processed and reviews this process every year.
2. The archiving policy must consider what data must be retained, for how long and why.

Security

1. CERC must ensure that personal data are stored securely using modern, up-to-date software.

2. Access to personal data must be limited to the staff who need it, and appropriate security must be in place to prevent the unauthorised sharing of information.
3. When personal data are deleted, this must be done securely so that the data are unrecoverable.
4. Appropriate back-up and disaster recovery solutions must be in place.

Security breaches

In the event of a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, CERC promptly assesses the risk to people's rights and freedoms and, where appropriate, reports the breach to the competent authorities.



CENTRE DE RECHERCHE SUR L'ANTI-CORRUPTION

 [cerccongo](https://www.facebook.com/cerccongo)

 [cerccongo](https://twitter.com/cerccongo)

 [cerccongo](https://www.linkedin.com/company/cerccongo)

 [cerccongo](https://www.instagram.com/cerccongo)

www.cerc.cd

32, Avenue CPA, Quartier CPA Mushi, Commune de Mont-Ngafula, Kinshasa, DRC

info@cerc.cd · +243 977 757 227

CERC is a registered non-governmental organisation (NGO) (Registration number: F.92/42579) and given Legal Personality by the Ministry of Justice: JUST/SG/20/21311/2021.

CERC holds Special Consultative Status with the United Nations Economic and Social Council (ECOSOC).