CBM Global Policy
Data Protection

May 2025

CBM Global Disability Inclusion
Van Heuven Goedhartlaan 13D, 1181 LE Amstelveen, Netherlands
https://cbm-global.org

Introduction and purpose

The General Data Protection Regulation (GDPR) is **a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU)**. The GDPR's primary aim is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business. The Data Protection legislation imposes obligations on Data Processors and Data Controllers regarding how they process sensitive personal data.

CBM Global is committed to complying with its obligations under the GDPR and to using GDPR as a framework guiding its approach to data protection worldwide. The purpose of this policy is to ensure CBM Global meets its statutory obligations as a Data Processor and/or a Data Controller.

This policy is **applicable worldwide to any CBM Global employee, consultant, volunteer or Board member** who is **engaged in activities and operations of CBM Global which involve the processing of personal data of individuals**, including the receipt of personal data from programme participants and community members collected by CBM Global partners relating to programme activities funded by CBM Global. CBM Global Members are encouraged to adopt the policy where no policy currently exists, and/or to ensure that any existing Member policies relating to Data Protection align with this policy.

Definitions

Anonymous data means that all the personal identifiable factors have been removed from data sets in such a way that there is no reasonable likelihood that the data subject could be identified or traced. Fully 'anonymised' data does not meet the criteria necessary to qualify as personal data. Data can be considered 'anonymised' when individuals are no longer identifiable.

Consent means any free, voluntary and informed decision that is expressed or implied and which is given for a specified purpose.

Child means any legal individual who has not yet attained majority.

Data controller means CBM Global staff or an individual that maintains processes or controls data.

Data processing means the way (personal) data is collected, registered, stored, filed, retrieved, used, disseminated, communicated, transferred and destroyed.

Data protection means the systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the collection, storage, use and disclosure of personal data.

Data subject means an individual that can be identified directly or indirectly by reference to a specific factor or factors. Such factors include a name, an identification number, material circumstances and physical, mental, cultural, economic or social characteristics that can be used to identify an individual.

Electronic record means any electronic data filing system that records (personal) data.

CBM Global staff means all persons who are employed by CBM Global, whether temporarily or permanently.

Non-personal data means any information that does not relate to an identified or identifiable data subject that is recorded by electronic means or on paper.

Personal data means any information relating to an identified or identifiable data subject that is recorded by electronic means or on paper.

Pseudonymisation of data means replacing any information which could be used to identify an individual with a pseudonym, or in other words, a value which does not allow the individual to be directly identified.

Third party means any natural or legal person, government or any other entity that is not party to the original specified purpose(s) for which (personal) data are collected and processed. The third party that agrees in writing to the transfer conditions outlined in the relevant Policy Statement shall be authorised to access and process personal data.

Vulnerable group means any group or sector of society, including children or adults-at-risk, that is at risk of being subjected to discriminatory practices, violence, natural disasters, or economic hardships.

Principles

CBM Global is committed to and will ensure **compliance with Articles 5.1 and 5.2 of the GDPR** which provide the following seven protection and accountability principles when processing personal data:

Lawfulness, fairness and transparency

Personal data must be obtained by lawful and fair means with the knowledge or consent of the data subject.

Purpose limitation

The purpose(s) for which personal data is collected and processed should be specified and legitimate and should be known to the data subject at the time of collection. **Personal data should only be used for the specified purpose(s)** unless the data subject consents to further use or if such use is compatible with the original specified purpose(s). Consent should only be obtained to achieve the purpose stated to the data subject.

Data minimization

Personal data sought and obtained **should be adequate, relevant and not excessive in relation to the specified purpose(s) of data collection and data processing**. Data controllers should take all reasonable steps to ensure that personal data are accurate and up to date.

Accuracy

Data maintained should be accurate and, where necessary, **kept up to date**. All CBM Global employees are required to proactively inform their HR focal point of any changes in their personal data. Reasonable steps should be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased, or rectified without delay.

Storage limitation

Personal data should be kept for as long as is necessary and **should be destroyed or rendered anonymous as soon as the specified purpose(s) of data collection and data processing have been fulfilled.** It may, however, be retained for an additional specified period, if required for the benefit of the data subject. The data controller must regularly review storage limitation.

Integrity and confidentiality

Confidentiality of personal data must be respected and applied to all the stages of data collection and data processing and should be guaranteed. All CBM Global employees, officers, Board members and individuals representing third parties who are authorised to access and process personal data are bound to confidentiality.

Accountability

The data controller is responsible for being able to demonstrate GDPR compliance with the above 6 principles.

Policy statements

Privacy rights for data subjects

CBM Global, as a data controller and/or a data processor, **recognises** **the privacy rights for data subjects**, as provided under GDPR, which aim to give individuals more control over the data they provide to CBM Global. CBM Global understands, recognises, upholds and **will ensure compliance with data subjects' rights as below**:

1. The right to be informed regarding the collection and further processing of their personal data
2. The right of access to any data held about them by CBM Global
3. The right to rectification – to have inaccurate data corrected
4. The right to erasure - to have information erased
5. The right to restrict processing of their data for direct-marketing purposes
6. The right to data portability - allows data subjects to obtain data that a data controller holds on them and to reuse it for their own purposes. Individuals are free to either store the data for personal use or to transmit it to another data controller.
7. The right to prevent processing that is likely to cause damage or distress to themselves or anyone else
8. The right to object to automated decision making and profiling

9. The right to know that their data will be destroyed after the purpose of collection and or processing has been obtained and/ or the data has been anonymised.

Accountability

To demonstrate CBM Global is compliant with the GDPR, it will:

- Maintain documentation of data collected, how it's used, where it's stored, which employee is responsible for it;
- Implement basic training to staff on GDPR and implement technical and organisational security measures;
- Inform CBM Global partner organisations regarding data protection obligations relating to programme activities funded by CBM Global in the collection of personal data and subsequent reporting;
- Request only necessary data (anonymised, pseudonymised or personal) from CBM Global partner organisations and will explain why the data is required;
- Have Data Processing Agreement contracts in place with third parties who process data for CBM Global;
- Appoint a Data Protection Officer (DPO).

Data Security

CBM Global will take all reasonable steps to ensure personal data, electronic or manual, is kept secure, both technically and organisationally, and should be protected by reasonable and appropriate measures against unauthorised modification, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer.

Security measures, as provided below, will be reviewed regularly, having regard to the technology available, the cost and the risk of unauthorised access:

- CBM Global shall ensure that personal data is stored securely using modern software that is kept up to date;
- Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of personal data;
- If personal data is deleted, this shall 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, **CBM Global shall promptly assess the risk and take immediate, appropriate, corrective action(s)** and shall meet GDPR Data Breach Reporting requirements.

All CBM Global employees are required to comply with CBM Global's Data Protection policy and ICS Guidelines, including system security policies and procedures.

Lawful purposes

In compliance with Article 6 of the GDPR, **CBM Global will process personal data only if one or more of the following conditions are met**:

- The data subject has provided specific, unambiguous consent to process the data;
- Processing is necessary to execute or to prepare to enter into a contract to which the data subject is a party;
- Data is required to be processed to comply with a legal obligation;
- Data is processed to protect the vital interests of a data subject e.g., to save somebody's life;
- Processing is necessary to perform a task in the public interest or to carry out some official function;
- CBM Global has a legitimate interest to process someone's personal data.

Consent

Consent must be obtained at the time of collecting data or as soon as it is reasonably practical thereafter. This includes consent obtained by partner organisations from programme participants and community members relating to programme activities funded by CBM Global. The condition and legal capacity of certain vulnerable groups and individuals should always be taken into account.

If exceptional circumstances hinder the achievement of consent, the data controller should, at a minimum, ensure that the data subject has sufficient knowledge to understand and appreciate the specified purpose(s) for which personal data are collected and processed.

CBM Global will adopt the following rules to establish what constitutes consent:

1. Consent must be freely given, specific, informed and unambiguous.
2. Requests for consent must be clearly distinguishable from the other, unrelated matters and presented in "clear and plain'' language.
3. Data subjects can withdraw previously given consent whenever they want, and CBM Global will honour their decision.
4. Children can only give consent with permission from their parent.
5. Documentary evidence of consent is to be maintained.
6. Where possible, consent should be recorded in writing.

Data transfer to third parties

Personal data will only be processed for employment-related purposes and in general will not be disclosed or transferred to third parties, except where required legally as part of CBM Global's regular activities or with the agreement of the employee. All personnel files are stored in the HR Department and employees who have access to these files ensure that they treat them confidentially and in accordance with the data protection principles listed above.

Access and Transparency

Data subjects are provided the opportunity to verify their personal data and would be provided with access insofar as it does not frustrate the specified purpose(s) for which

personal data are collected and processed. CBM Global provides a general policy of openness towards the data subject about developments, practices and policies with respect to personal data.

Responsibilities

CBM Global management will ensure that this policy is issued to all employees, consultants, volunteers and board members and obtain their confirmation of understanding and an undertaking to comply with this policy.

Employees that have access to personal data because of the nature of their role should seek approval before sharing it with anyone else by using this email address: dpo@cbm-global.org

If an employee is sent, in error, confidential or personal information s/he should immediately delete the information without storing it or disseminating it and should immediately alert the sender. The same process applies if an employee is given access by mistake to confidential or personal information.

It is the responsibility of **the Country Team** to ensure that partner organisations understand the data protection obligations of this policy in relation to programme activities funded by CBM Global and that partners obtain consent for personal data gathered (e.g. to meet donor compliance or audit requirements) from programme participants and community members.

If an employee receives project reporting from a partner organisation which includes confidential or personal information which has not been agreed upon as required personal data s/he should immediately delete the information without storing it or disseminating it, and should immediately alert the sender, stating that such reporting must be anonymised.

All employees, Board members, volunteers and consultants and relevant related parties can raise issues of concern or observed non-compliance to their manager or the Data Protection Officer.

Failure to comply with this policy may result in disciplinary and/or legal proceedings up to and including, as appropriate, dismissal, termination of contract or termination of board terms.

Complaints

All employees, Board members, volunteers and consultants have a right to lodge a complaint to the Data Protection Officer (dpo@cbm-global.org) if they believe their rights under the Data Protection legislation are not being protected by CBM Global. Serious issues of continued non-compliance can be escalated to their national Data Protection Commissioner (independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law in their country). The DPO of CBM Global will co-operate with DPOs of individual Member organisations, if necessary and appropriate.

Key references and supporting documents

All documents mentioned above are available to CBM Global Federation staff on Global Connect. Documents that are relevant for external audiences can be found on www.cbm-global.org.

- ICS Guidelines