

Data protection and Cybersecurity Policy

DATA PROTECTION AND CYBERSECURITY POLICY

Member:	• all board members/trustees, board committee members • all association employees, secondees, interns and volunteers; and • all consultants/contractors/suppliers (including internal consultants with an association email address) • all association partners
Title:	Data Protection and Cybersecurity Policy
Document type:	Policy
Date/version:	September 2024 / Version 1
Classification:	General Distribution
Author:	Adil Murat Vural, Head of Management Board
Owned by:	Management Board
Reviewed and approved by:	Management Board
Next review date:	September 2025

1. Introduction

The Climate Change and Food Security Association (CCFSA) recognizes the critical importance of protecting personal data and sensitive information in its possession. This Data Protection and Cybersecurity Policy outlines CCFSA's commitment to ensuring the confidentiality, integrity, and availability of all data it collects, stores, and processes. This policy complies with relevant data protection regulations and best practices in cybersecurity.

2. Scope

This policy applies to all CCFSA members, staff, volunteers, contractors, and any other individuals who handle data on behalf of the organization. It covers all data, including personal data of individuals (e.g., donors, beneficiaries, partners) and organizational data (e.g., financial records, research data).

3. Data Protection Principles

CCFSA adheres to the following data protection principles:

- **Lawfulness, fairness, and transparency:** Data will be processed lawfully, fairly, and in a transparent manner.
- **Purpose limitation:** Data will be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data minimization:** Data collected will be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy:** Data will be accurate and, where necessary, kept up to date.
- **Storage limitation:** Data will be 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.
- **Integrity and confidentiality:** Data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.
- **Accountability:** CCFSA is responsible for and able to demonstrate compliance with the above principles.

4. Cybersecurity Measures

CCFSA implements the following cybersecurity measures to protect data:

- **Access control:** Restricting access to data based on roles and responsibilities, using strong passwords and multi-factor authentication.
- **Network security:** Implementing firewalls, intrusion detection systems, and other security measures to protect the network from unauthorized access.
- **Data encryption:** Encrypting sensitive data both in transit and at rest.
- **Data backups:** Regularly backing up data to ensure recovery in case of data loss.
- **Software updates:** Keeping all software, including operating systems and applications, up to date with the latest security patches.
- **Vulnerability management:** Regularly assessing and addressing security vulnerabilities.
- **Incident response:** Establishing procedures for responding to and managing security incidents.

5. Data Subject Rights

CCFSA respects the rights of data subjects under relevant data protection regulations, including the right to:

- **Access:** Request access to their personal data.
- **Rectification:** Request correction of inaccurate or incomplete personal data.
- **Erasure:** Request deletion of their personal data.
- **Restriction of processing:** Request restriction of processing of their personal data.
- **Data portability:** Receive their personal data in a structured, commonly used, and machine-readable format.
- **Object:** Object to the processing of their personal data.

6. Employee Training and Awareness

CCFSA provides regular training and awareness programs to employees on data protection and cybersecurity best practices.

7. Policy Review and Updates

This policy will be reviewed and updated periodically to ensure it remains relevant and effective.

8. Contact Information

For any questions or concerns regarding this policy, please contact the CCFSA Data Protection Officer at

9. Data Breach Notification

In the event of a data breach, CCFSA will promptly notify affected individuals and relevant authorities as required by applicable laws and regulations.

10. Specific Considerations for Climate Change and Food Security Data

CCFSA recognizes the sensitive nature of data related to climate change and food security. The organization will take extra precautions to protect such data, including:

- **Anonymization and pseudonymization:** Implementing techniques to de-identify personal data whenever possible.
- **Data sharing agreements:** Establishing clear data sharing agreements with partners and collaborators.
- **Ethical considerations:** Ensuring that data collection and processing activities are conducted in an ethical and responsible manner, considering potential impacts on vulnerable communities.

This policy provides a framework for CCFSA's data protection and cybersecurity efforts. The organization is committed to continuously improving its practices to ensure the highest level of protection for all data in its care.