

# CODE OF CONDUCT

REVISED SEPTEMBER 2025



PHOTO: KIRSTEN ADLER

*This is a translation of the Danish original.  
In case of doubt or discrepancy, the Danish version shall prevail.*

# Contents

<b>1. Introduction.....</b>	<b>3</b>
1.1 Background.....	3
1.2 A dynamic document.....	3
1.3 Target groups and terminology.....	3
1.4 External communication.....	3
1.5 Prevention of breaches.....	4
1.6 Consequences of breaches.....	4
1.7 CISU's foundation and values.....	4
1.8 Management of CISU.....	4
1.9 Quality Assurance.....	4
<b>2. Ethical principles and guidelines.....</b>	<b>5</b>
2.1 Fundamental Ethical Principles.....	5
2.2 Application of the Ethical Principles.....	5
<b>3. Safeguarding.....</b>	<b>7</b>
3.1 Definitions.....	7
3.2 Prevention of sexual harassment, exploitation and abuse of power.....	7
3.3 Reporting sexual exploitation and abuse of power.....	8
<b>4. Legal principles and guidelines.....</b>	<b>9</b>
4.1 Legal basis.....	9
4.2 Core legal principles.....	9
4.3 Principles for processing personal data.....	10
4.4 Consequences for work processes.....	11
<b>5. Anti-corruption, irregularities and reporting.....</b>	<b>12</b>
5.1 Target group.....	12
5.2 Objective: to avoid corruption, fraud and misuse altogether.....	12
5.3 Definitions.....	12
5.4 CISU.....	13
5.5 Member organisations.....	13
5.6 Grant holders under CISU's funding schemes.....	13
5.7 Reporting of irregularities and suspicion of corruption.....	14
<b>6. Security.....</b>	<b>15</b>
6.1 General security.....	15
6.2 Security on international travel.....	15
<b>7. Complaints to CISU.....</b>	<b>16</b>
7.1 Introduction of principles.....	16
7.2 Complaints about processing in CISU's grant assessment system (Grant Complaints) [K1].....	17
7.3 Complaints about internal matters and/or CISU staff/management/board members [K2].....	18
7.4 Complaints about grant holders and partners in CISU-funded activities [K3].....	19
7.5 Whistleblower Scheme.....	20
<b>8. Anti-terror.....</b>	<b>21</b>
8.1 Introduction.....	21
8.2 CISU's requirements and monitoring.....	21
8.3 CISU's anti-terror initiatives and capacity building.....	21
8.4 CISU's anti-terror screening.....	21



# 1. Introduction

## 1.1 Background

This Code of Conduct brings together the most important principles, guidelines and contingency plans that CISU applies in its daily work.

The code is based on our shared values and many years of experience with responsible and transparent grant management and capacity development. Transparency and integrity are the fundamental principles in everything we do. The code helps ensure that we can perform our tasks effectively and reach the goals we have set ourselves.

We have aimed to write in a language that is easy to understand. At the same time, the code also serves as a legal and administrative framework for our work. For that reason, some sections are necessarily more technical and detailed.

Everyone in and around CISU is welcome to suggest how we can further improve the code – and its practical application.

## 1.2 A dynamic document

This Code of Conduct is a living document that may be adjusted on an ongoing basis. Changes may occur when new knowledge, new regulations, altered needs or changes in our context arise.

Every year, we review the Code of Conduct to assess whether updates are needed. Substantial changes must be approved by the board. As part of the annual monitoring process, the board is informed of cases that fall within the scope of the code.

When drafting the most central parts, legal advice has been obtained, and we continuously assess whether additional legal input is required.

## 1.3 Target groups and terminology

The primary target group for the Code is CISU's own organisation: the board, secretariat staff (including management),

external consultants during contract periods, grant consultants, and members of CISU's assessment committees and steering committees. In the code, the term "CISU" refers to this group. Individuals covered by the code confirm through their contracts and agreements that they are aware of its content and will comply with it.

The secondary target group comprises all other actors that have a contractual relationship with CISU. This includes individuals, institutions, businesses and organisations with which CISU cooperates, for example those who:

- receive funds from CISU to carry out a task
- provide a service or deliverables
- receive funds to implement awareness-raising activities, development projects and/or humanitarian efforts

The provisions of this Code of Conduct apply directly to these actors when specified in agreements, grant contracts or similar. The same applies where Danish legislation or other regulatory frameworks (e.g. criminal law or liability law) make it relevant.

Indirectly, "other stakeholders" are also a target group, as they encounter CISU's principles through our materials, dialogue and capacity building. In this code, the term "other stakeholders" refers to this whole group.

## 1.4 External communication

When reporting to donors, CISU's Code of Conduct forms an important part of the documentation. Cases of corruption are published on the Ministry of Foreign Affairs' website in accordance with applicable rules and GDPR.



PHOTO: KIRSTEN ADLER

### 1.5 Prevention of breaches

CISU's management actively works to ensure that all those covered by the code are aware of their responsibilities. We inform, train and guide key staff so that they can act in accordance with the principles and support others in doing the same.

### 1.6 Consequences of breaches

Violations of the Code of Conduct may result in consequences depending on the nature and seriousness of the case. Consequences may range from guidance and reprimands to termination of cooperation, reporting to the police, or claims for compensation.

If CISU finds that individuals, companies or organisations have seriously violated the Code of Conduct, we may impose various sanctions, including:

- For secretariat staff and contracted actors: disciplinary measures such as warnings, dismissal or summary termination

- For member organisations: suspension of membership
- For grant holders and suppliers: termination of contractual relations, possibly with immediate effect
- In criminal matters: reporting to the police
- In cases of incurred loss: filing a claim for damages

### 1.7 CISU's foundation and values

CISU is a membership-based civil society organisation that works on the basis of statutes and strategies adopted by the annual general assembly and the board. Our work supports capacity development, grant management and international development and humanitarian efforts, with respect for human rights and the UN Sustainable Development Goals. As an organisation, CISU represents the interests of its member organisations in strengthening civil society participation.

### 1.8 Management of CISU

The management of CISU is described in the statutes. The secretariat is led by a secretariat management team. The board holds strategic responsibility for CISU, as described in the organisation's 'The Board's Governance of CISU, including Rules of Procedure'.

### 1.9 Quality Assurance

CISU has extensive systems, guidelines and procedures to ensure quality in its work. These are continuously adjusted by working groups and group coordinators, with follow-up by management and the board.

Grant management is based on transparent and professional processes, which are approved by donors and supported by this Code of Conduct.

### CISU'S CORE VALUES (ADOPTED 2016)

These values underpin our daily work. They provide the framework for how we view the world and engage in relations. Our credibility depends on our ability to translate these values clearly into practice.

- **Diversity:** We strive for a wide range of approaches to civil society work, as diversity of approaches and actors is characteristic of a well-functioning civil society
- **Transparency:** We seek transparency in all our actions and decisions
- **Accountability:** We take responsibility for our own actions and decisions and expect the same of others
- **Participation:** We provide equal opportunities for everyone to engage, as all people have something valuable to contribute
- **Respect:** We meet people where they are and support them in working towards their own goals. We allow our views and perspectives to be challenged and learn in the process
- **Collaboration:** We work broadly with others, as it is an inspiring, necessary and constructive path to sustainable results
- **Voluntarism:** We create space for voluntary involvement in civil society, as free will and voluntarism are the driving forces of committed civil society work



## 2. Ethical principles and guidelines

### 2.1 Fundamental Ethical Principles

CISU's Ethical Principles are built on CISU's values: diversity, transparency, accountability, participation, respect, collaboration and voluntarism. These values form the foundation of our work and reflect a human rights-based approach, including the *PANT principles* (*Participation, Accountability, Non-discrimination and Transparency*). The following sections elaborate on selected values and show how they are translated into ethical principles in our work.

#### 2.1.1 Transparency and confidentiality

CISU emphasises openness and transparency in cooperation with member organisations, donors, partners, the press and the public. Our starting point is that information should be shared as openly as possible. At the same time, we have a clear obligation to protect confidential information – both concerning personal matters, privacy, and sensitive data we receive through, for example, advisory services, courses or other activities. The rules on transparency and confidentiality are set out in CISU's legal guidelines and supplemented by our policies on data protection and the handling of personal data.

#### 2.1.2 Good cooperation and conduct

CISU strives for cooperation based on respect, recognition and a constructive tone. This applies in relations between colleagues, between management and staff, within the board and assessment committees, as well as in contact with members, partners, the press and other stakeholders.

#### 2.1.3 Non-discrimination

In CISU, we treat all people with respect. We do not accept any form of discrimination – neither in our internal work nor in our external relations. This means that we do not discriminate on the basis of gender, race, ethnic origin, sexual orientation, religion, culture, age, education, social status or nationality.

#### 2.1.4 Zero tolerance of abuse of power, position or resources

CISU does not accept that anyone uses their position in the organisation to advance personal interests or to exert pressure on other individuals, companies or organisations. We also do not accept CISU's resources, premises or equipment being used for private purposes without permission.

To prevent abuse and ensure equality in all relations, we have systems and procedures to protect against both discrimination and misuse of power. Here we also refer to our separate section on safeguarding.

#### 2.1.5 Actual and potential conflicts of interest

In CISU, we work to avoid situations where personal interests may conflict with the organisation's interests – or where there may be an impression that such a conflict exists. Private interests can include any kind of advantage benefiting oneself, family, friends, business associates or organisations with which one is affiliated.

### 2.2 Application of the Ethical Principles

#### 2.2.1 In the organisation's daily work

##### *Impartiality:*

Everyone in CISU is responsible for informing management – or the board – of any actual or potential conflicts of interest. This also means declaring oneself disqualified if there is any doubt about impartiality.

- For employees, members of assessment committees and grant consultants, CISU's management decide in cases of doubt
- For the management team itself, the chairpersons decide in cases of doubt
- For the chairpersons, the board decide in cases of doubt

##### **GIFTS AND BENEFITS:**

We must neither directly nor indirectly give, receive or facilitate gifts or other benefits if they could influence our impartiality or the performance of our tasks. However, minor tokens such as meals or ordinary gifts in connection with birthdays or anniversaries are acceptable,

If employees receive small gifts or tokens of appreciation in connection with their work (e.g. food and drink after giving a presentation), these are considered to belong to the workplace and are therefore shared collectively among staff.

A more detailed description of how we handle corruption and irregularities is found in CISU's Anti-Corruption Policy (see section 5).

### 2.2.2 Reporting serious concerns

If anyone in CISU becomes aware of – or has a reason to suspect – serious concerns or circumstances, the information must immediately be passed on to CISU's management.

Examples of such concerns may include:

- Sexual exploitation
- Abuse of power
- Corruption

This applies both internally within CISU and in relation to our grant holders or their partners.

All options for reporting concerns, providing feedback and filing complaints are described in section 7. This section also sets out CISU's guidelines for protecting individuals who report as whistleblowers – i.e. when reporting serious matters in confidence and with protection against negative consequences.

### 2.2.3 Business travel

When CISU staff travel abroad for work purposes, we commit to the same ethical and professional standards that we expect of our member organisations, grant hol-

ders and their partners. In other words, we must demonstrate the behaviour we work to promote globally.

However, it is important to emphasise that our own safety always comes first. We never compromise if exposed to extortion or threats. In such cases, the incident must be reported immediately to management so it can be handled appropriately and safely.

PHOTO: KIRSTEN ADLER



# 3. Safeguarding

## 3.1 Definitions

*Safeguarding* means protecting people's health, well-being and rights and ensuring that everyone can live free from the risk of harm, abuse and neglect. It is a shared responsibility to safeguard children, young people and adults.

In international contexts, the abbreviation *PSEAH* is often used, which stands for *Preventing Sexual Exploitation, Abuse and Harassment*.

CISU has a zero-tolerance policy towards any form of sexual harassment, exploitation or abuse of power. This applies both internally in the organisation and in relation to all individuals and actors we work with – including member organisations, grant holders and their partners. Our approach is in line with Danish criminal law.

With respect for people's dignity and right to safety, CISU actively works to protect everyone who comes into contact with the organisation. Our work is based on both prevention and response: we implement initiatives that prevent violations and act immediately in cases of suspicion or confirmed incidents. All cases are followed up so that sanctions can be applied and support and learning offered, while ensuring protection of those involved.

Responsibility lies with CISU's management, who work closely with an internal Code of Conduct group, a staff representative and a health and safety representative. The aim is to ensure effective and up-to-date policies and practices, so CISU can best protect affected individuals while ensuring that all parties have the necessary legal safeguards.

## 3.2 Prevention of sexual harassment, exploitation and abuse of power

### 3.2.1 Within CISU

CISU supports an open and safe working environment where everyone is treated with respect and where the organisation's ethical guidelines are followed. All employees share responsibility for contributing to the development and maintenance of this environment.

Management is responsible for ensuring a safe working environment in which no one is exposed to harassment, exploitation or abuse. Management ensures that all employees are aware of their rights and duties, and that CISU's safeguarding guidelines are known and understood.

Management must always ensure that staff have the necessary competences through capacity building, exchange of experience and the use of external expertise when needed.

### 3.2.2 Employees, board and members of grant assessment systems

Safeguarding is an integral part of all recruitment and appointment processes at CISU. Job advertisements always refer to the Code of Conduct, and where relevant, information about safeguarding experience may be obtained from previous workplaces.

- The newly elected board is introduced to the Code of Conduct at their constitutive meeting and as part of the annual monitoring process
- New employees and members of assessment committees are introduced to safeguarding as part of the onboarding process

- Safeguarding may be discussed in annual staff performance reviews, annual assessment system reviews and annual management reviews
- Safeguarding is also included in CISU's workplace assessment surveys.

### 3.2.3 Other actors

CISU also works to prevent sexual exploitation and abuse of power in collaboration with external actors. This is done through information, capacity building, contracts and cooperation agreements.

- All member organisations, grant holders and partners are informed that CISU has a zero-tolerance policy
- Safeguarding is included in all CISU contracts, and violations may lead to immediate termination of agreements
- CISU offers courses and organisational development workshops that support member organisations in establishing their own safeguarding procedures
- CISU recognises that some groups are particularly vulnerable, for example children and women in fragile or humanitarian contexts where rights are under pressure. We therefore place special focus on the protection of these groups

CISU is also HQAI-verified against the *Core Humanitarian Standards (CHS)*, which supports our safeguarding work in CISUs different funding schemes.



### 3.3 Reporting sexual exploitation and abuse of power

CISU takes all reportings of sexual exploitation and abuse of power seriously and investigates them thoroughly. Reporting can be done through the complaints system (see section 7).

#### 3.3.1 Internal reporting at CISU

It is part of CISU's working culture that everyone has a duty to act if they experience or observe behaviour that goes against our Ethical Principles. Any employee who becomes aware of matters that may constitute sexual exploitation or abuse of power must report it.

Reports may be made to:

- A member of CISU's management team
- A staff representative or health and safety representative
- A trusted colleague
- Via CISU's complaints system (with the option of anonymity, see section 7)

#### 3.3.2 External reporting

Anyone who observes sexual harassment, exploitation or abuse of power in connection with CISU's work – either within the organisation itself or among member organisations, grant holders and partners – may report the case. This can be done anonymously and confidentially through CISU's complaints system. Individuals who have

personally experienced such violations may report directly or through someone they trust.

#### 3.3.3 Follow-up

CISU takes all reports seriously and investigates them thoroughly. In cases of sexual abuse or abuse of power, affected persons are offered qualified crisis support as quickly as possible. This may include counselling, psychological assistance or other support necessary, with CISU covering the costs.

CISU provides information about received and processed complaints in the annual report and whenever otherwise required. In any communication, CISU balances the need for transparency with respect for legal safeguards and data protection rules.

PHOTO: KIM JENSEN, CISU



# 4. Legal principles and guidelines

The legal principles guiding CISU's work are summarised below.

## 4.1 Legal basis

CISU is a private organisation and as such not legally bound by the Danish Public Administration Act (*Forvaltningsloven*) or the Danish Access to Public Administration Files Act (*Offentlighedsloven*). At the same time, we manage significant public funds through grants from the Ministry of Foreign Affairs. The public can therefore rightly expect us to follow the principles of good administrative practice (i.e. impartial, transparent and proper processing of applications and grants).

CISU's board has therefore decided that we will operate as if we were subject to the Danish Access to Public Administration Files Act (*Offentlighedsloven*) and the Danish Public Administration Act (*Forvaltningsloven*) and that we will apply the principles of good administrative practice in our work.

CISU, like other organisations, is covered by the General Data Protection Regulation (GDPR) and the Danish Data Protection Act.

For the sake of our legitimacy, we wish to be as open as possible in response to requests for access to information relating to our application and grant processing, insofar as confidentiality and data protection rules allow.

## 4.2 Core legal principles

CISU is not a public authority, but we have chosen to follow a number of core principles from the Danish Public Administration Act (*Forvaltningsloven*) and the Danish Access to Public Administration Files Act (*Offentlighedsloven*), because we administer public funds. In addition, we highlight relevant principles from the GDPR.

### 4.2.1 Duty of investigation (official principle)

*(Not based on specific legislation, but on unwritten legal custom)*

We are responsible for ensuring that all necessary information is obtained so that we can make the most accurate decision. This means we cannot reject an application solely due to missing information, such as basic data about a partner. Instead, we must ask the applicant to provide the required information within a reasonable deadline. If the information is not then submitted, we may reject the application.

Clearly incomplete applications, or those falling outside the scope of the guidelines, can be rejected outright, as the ability to formulate and prepare a project is part of the assessment of the applicant's capacity.

### 4.2.2 Principle of impartiality

*(Forvaltningsloven, Chapter 2)*

The processing of applications must be impartial. If an employee or decision-maker has personal or financial interests in an application, they are disqualified and may not participate in the processing or decision.

### 4.2.3 No rigid-rule-application

*(Practice based on court rulings)*

The fund guidelines must always be applied with due discretion. To ensure consistency when processing applications, we develop internal rules and practices – both written and unwritten. They ensure a smooth and fair processing of applications.

However, these internal rules must never become so rigid that they replace individual discretion. Each application must be assessed specifically against the guidelines, and there must always be room for atypical cases.

### 4.2.4 Principle of proportionality

*(Not based on specific legislation, but on unwritten legal custom)*

This principle means we may only impose requirements on applicants that are proportionate to the application. For example, our demands for the level of detail, documentation etc. in an application must be proportionate to the amount being applied for.

The principle does not apply the other way round: our administrative workload is not required to be proportionate to the application. However, we may reject applications by reference to our resources, e.g. when processing clearly incomplete applications.

### 4.2.5 Hearing of the party concerned

*(Forvaltningsloven, Chapter 5)*

If new information is added to an application – for example, a consultation response from an embassy – which is unfavourable to the applicant and of significant importance to the decision, the applicant has the right to be heard and comment before a decision is made. In such cases, CISU sends the relevant information to the applicant, who must respond in writing within a reasonable deadline.

### 4.2.6 Duty to take notes

*(Offentlighedsloven § 13)*

If we receive oral or otherwise informal information about facts that are significant for a decision, we must record it and place a note in the application system. This does not apply if the information already appears in the application documents. Notes become part of the application and are subject to right of access to information.

### 4.2.7 Duty to record

*(Offentlighedsloven § 15)*

All documents relevant to a decision must be recorded with the date of receipt or dispatch. Recorded documents are subject to right of access to information.

### 4.2.8 Duty to provide guidance

(*Forvaltningslovens § 7*)

We are obliged to guide applicants about, for example, application forms, deadlines and guidelines. This duty does not extend to actual advice about project design or application wording – but such advice may be offered as a service to member organisations.

### 4.2.9 Duty to provide reasons for rejections

(*Forvaltningslovens, chapter 6*)

Rejections (in whole or in part), or approvals with conditions/reservations, must be justified in writing. The justification must refer to the relevant rules (typically in the fund guidelines). In cases involving due discretion, we must state the main considerations underlying the final decision. Approvals without conditions do not require justification.

### 4.2.10 Duty of confidentiality

(*Forvaltningslovens, chapter 8, and Danish Penal Code, §152*)

We are bound by confidentiality regarding information about individuals as well as internal and financial matters of private companies/organisations – including where disclosure could damage, for example, a partner organisation in another country. This duty of confidentiality also applies towards public authorities, such as the Ministry of Foreign Affairs.

As a private organisation, we are not covered by *Forvaltningsloven §28* on disclosure to other authorities. CISU generally does not disclose personal data to authorities unless required by law.

### 4.2.11 Right of access to information

The public and parties to an application generally have the right of access to information:

**Access under *Offentlighedsloven* (Chapter 2):** Anyone may request access, regardless of whether they are a party. This generally covers all documents sent to or created by us during processing.

Important exceptions include:

- a) Internal working documents
- b) Information on private matters (including financial matters)
- c) Information we are not permitted to disclose under GDPR

Internal documents may, however, be included if they contain significant factual information not found elsewhere, or if they have been shared externally and are therefore no longer internal.

### **Extended access to information (*Offentlighedsloven §14 and Forvaltningsloven §10*:**

We must consider granting broader access than legally required, unless there are reasons not to. If nothing prevents disclosure, documents/information should be released. *r dokumenter/ oplysninger udleveres.*

**Access under *Forvaltningsloven* (Chapter 4):** This right applies only to parties to an application.

Parties are entitled to access all documents, including internal documents, if they contain significant information or assessments not available elsewhere, or if they were created as part of the duty to take notes.

Because we voluntarily follow the principles of good administrative practice (and not because of direct legal obligation), we may have to withhold access to personal data if disclosure is not authorised under GDPR.

## 4.3 Principles for processing personal data

(*GDPR, art. 5*)

CISU is covered by the General Data Protection Regulation (GDPR). This means that all processing of personal data follows these principles:

- We only process personal data when lawful and fair, and we are as open as possible with the individual concerned. We provide clear information about our processing
- We collect and process personal data only for clear and legitimate purposes. If there is no relevant purpose, we do

not collect the data – and if the purpose ceases, we delete it

- Data collected for one purpose is not subsequently used for another purpose incompatible with the original
- We collect and process only the personal data that is necessary and relevant for the stated purposes – and we limit the scope to what is sufficient
- We strive to ensure that personal data is correct and up to date. If data proves to be incorrect, we rectify or delete it
- We do not store personal data longer than necessary. Once the purpose is fulfilled and there is no longer a basis for retention, we delete it securely
- We protect personal data against unauthorised access – including internally – as well as against accidental loss, destruction or damage, and we process it securely.

### 4.3.1 Processing of ordinary personal data

(*GDPR, Article 6: "Legal basis"*)

We process personal data only when authorised by the GDPR, typically:

- Consent (voluntary, specific, informed and unambiguous)
- Contract (necessary for entering into/ fulfilling an agreement or processing an application)
- Legal obligation
- Legitimate interest (where the interests of the data subject do not outweigh)

### 4.3.2 Processing of special categories of personal data

(*GDPR, Article 9: "Sensitive data"*)

Special categories (e.g. race/ethnicity, political/religious beliefs, trade union membership, genetic/biometric data, health, sexual life/orientation) are generally not collected.

If, in exceptional cases, there is a legitimate and relevant purpose, we may only process them if, for example:

- There is explicit consent
- The processing is necessary for labour, health or social law obligations based on law/collective agreement
- The processing is necessary to establish, exercise or defend legal claims



### *Civil registration numbers (CPR):*

These are only processed when:

- Required by law
- Conditions for processing special categories are fulfilled
- There is consent

### **4.3.3 Rights of data subjects**

(GDPR, art. 12-23)

Individuals whose data we process have rights, including:

- To be informed about our processing
- To access their own data
- To have incorrect data rectified
- To have data deleted in certain cases
- To restrict processing in certain cases
- To data portability (provision in a structured, machine-readable format)
- To object to processing (absolute right in cases of direct marketing)
- To withdraw consent
- To complain to the Danish Data Protection Authority

We assist and facilitate the exercise of these rights and respond as quickly as possible and no later than within one month.

## **4.4 Consequences for work processes**

### **4.4.1 General rights of access to information**

We are committed to maximum transparency regarding rights of access to information, while at the same time complying with GDPR. This may mean that we cannot disclose personal data, even if it would otherwise fall under rights of access to information.

- **Access for parties to an application (Forvaltningsloven):** We provide all documents – including relevant internal documents, notes, emails etc. – if they contain significant information or relevant assessments not available elsewhere.
- **Access under Offentlighedsloven:** Requests often concern documents from application processing and grant management – not necessarily advisory and training activities.

Openness is balanced against confidentiality (protection of applicants' financial interests) and data protection rules. Applications and annexes are generally covered, but personal data is excluded as required by law (typically by redaction before disclosure).

- **Extended access:** We always consider whether we can provide more information than legally required, unless something prevents it.
- **Deadlines:** Access must be granted as quickly as possible and within 7 working days, unless the scope/complexity of the case requires more time.

CISU informs affected parties when access is granted.

### **4.4.2 Access to information in operations and administration**

Internal accounts, expense vouchers etc. are covered by the right of access under Offentlighedsloven (with the usual exceptions).

### **4.4.3 Access to information in the grant process**

All communication between grant consultants and assessment committees/members is covered by access rights under either Forvaltningsloven or Offentlighedsloven. The same applies to communication between grant consultants and secretariat staff as part of the application processing – including emails and notes based on oral information.

Internal documents (communication within the assessment committee or among grant consultants) are not covered by access rights.

### **4.4.4 Confidentiality**

Applications and annexes are subject to confidentiality if they contain personal or sensitive information about applicants or partner organisations. The same applies to information from training and advisory services, unless included specifically in application processing.

Disclosure may take place only with prior written consent from the organisation – unless release is required under an access request.

### **4.4.5 Confidentiality towards the Ministry of Foreign Affairs**

CISU staff are bound by confidentiality in relation to the Ministry of Foreign Affairs and other authorities. We do not disclose information about member organisations/applicants that could harm their relationship with the authority, unless this is part of agreed procedures in case processing.

Information subject to access rights under Offentlighedsloven can generally be disclosed to relevant authorities.

### **4.4.6 Duty to take notes in the grant process**

Oral information received by grant consultants during the process is subject to the duty to take notes. The same applies to oral information given at assessment committee meetings when significant for the decision. The committee's discussions themselves are not included.

### **4.4.7 Duty of investigation**

Grant assessment consultants have both the right and the duty to obtain missing information so that the best possible decision can be made. Information may be obtained from applicants or – in the case of factual matters – from secretariat staff (e.g. whether an applicant has received advice, but not the content of the advice).

### **4.4.8 Processing of personal data**

We process personal data in accordance with GDPR and the Data Protection Act and also CISU's [Privacy Policy](#).

PHOTO: JACOB CRAWFURD



# 5. Anti-corruption, irregularities and reporting

## 5.1 Target group

CISU's Anti-Corruption Policy sets out our principles for preventing and addressing corruption, fraud and misuse. The policy applies:

- To CISU as an organisation
- To all grant holders under CISU's funding schemes
- To some extent also to other actors that CISU works with

## 5.2 Objective: to avoid corruption, fraud and misuse altogether

CISU does not accept any form of corruption, fraud or misuse, whether internally in the organisation, among partners, member organisations or grant holders under CISU's funding schemes.

We work actively with:

- **Prevention**, to minimise the risk of irregularities
- **Follow-up and monitoring**, to ensure suspicion or confirmed cases are handled consistently

We recognise that Danish civil society organisations often operate in countries where social and economic conditions may make corruption more widespread. We therefore expect our member organisations, grant holders and their partners to do their utmost to avoid and prevent corruption, even if they may involuntarily be affected by the problem.

CISU considers prevention to be the most important area of effort. The goal is to avoid irregularities – but if they nevertheless occur, we must limit the consequences and ensure adequate and reasonable follow-up, proportionate to the seriousness of the case.

Prevention is closely linked to the development of legitimate, transparent and democratically controlled organisations in recipient countries. This means, for example, that management and staff are held accountable by boards, members and target groups.

## 5.3 Definitions

**Corruption** is understood as: abuse of entrusted power and resources for personal gain. Personal gain may benefit oneself, but also family, friends, networks or other platforms that strengthen one's position

**Misuse of funds** can take many forms, for example:

- Fraud in connection with audits
- Deliveries not agreed upon
- Incorrect prices or equipment
- False invoices for staff or equipment
- Bribery or acceptance of gifts
- Misuse of resources or business travel
- Theft

**Abuse of entrusted power** can also take many forms, for example:

- Psychological, physical or sexual harassment
- Discrimination
- Unjustified allocation of privileges
- Abuse of relationships in connection with recruitment or other decisions

### 5.3.1 Scope

This section focuses primarily on misuse of funds. Other parts of the Code of Conduct address related issues such as abuse of power and discrimination.

## 5.3.2 Corruption in practice

There is no single clear definition of corruption. Inspired by the practice of the Ministry of Foreign Affairs, CISU considers the following actions to constitute corrupt or dishonest practices (the list is not exhaustive):

- **Fraud:** Deliberate actions for personal gain, e.g. extortion, collusion, nepotism (favouritism towards family/friends), theft, embezzlement, forgery, inflated prices
- **Corruption:** Offering or receiving payments beyond normal fees in exchange for special services or faster case processing
- **Misuse of funds:** Using money or assets (e.g. vehicles, phones) for purposes other than the project, or failing to maintain assets
- **Serious irregularities:** For example, inadequate bookkeeping, missing or delayed financial reporting to partners/donors, or other management failures
- **Acceptance of gifts or services:** It is not permitted to request or receive gifts that could influence work or decisions. Only purely symbolic gifts (e.g. pens or calendars) are acceptable – never valuable gifts, even if given to family members
- **Secrecy or concealment:** Withholding relevant information or possible conflicts of interest, e.g. close family ties, shareholdings or joint ownership in companies/organisations one collaborates with.

### 5.4 CISU

CISU must neither actively nor passively engage in corruption, bribery or fraud, as defined above.

Regardless of local customs or traditions, CISU never compromises on the organisation's integrity. This means that we neither in Denmark nor abroad give, facilitate, request or accept gifts or services of more than symbolic value that could affect our judgement or impartiality.

### 5.5 Member organisations

CISU actively works to prevent member organisations and their partners – regardless of local circumstances – from participating in corruption or bribery in any way. This also applies in countries where such practices may be widespread.

We support member organisations and their partners by:

- Sharing perspectives, knowledge and methods to prevent corruption, fraud and misuse

- Offering advice, courses and tools
- Providing materials through, for example, our website

CISU also helps member organisations and grant holders to clarify suspicions and act quickly and appropriately in cases of confirmed corruption, fraud or misuse. This is done through counselling, sparring, assistance with reporting, and in cooperation with the Ministry of Foreign Affairs, including possible support for legal clarification.

We regard it as good practice and a sign of organisational strength when an organisation that, unintentionally and without intent, becomes involved in corruption or bribery, is open about its experience and immediately takes the necessary steps to address the situation.

### 5.6 Grant holders under CISU's funding schemes

All grant holders under CISU's funding schemes are obliged to manage funds in accordance with the specific fund guidelines and the Ministry of Foreign Affairs'

requirements. This includes, among other things, the duty to prevent and counter corruption, fraud and misuse.

- All grant holders must sign to confirm that they follow the Ministry of Foreign Affairs' and/or the EU's anti-corruption clauses
- If there is a justified suspicion or confirmed case of theft, fraud, corruption, misuse or other irregularities, the Danish organisation is obliged to report this to CISU within 14 days.

CISU is obliged to act actively on all information indicating fraud, misuse of funds or corruption. We do this in loyal cooperation with organisations, so that grant holders and member organisations can confidently seek advice and guidance from us – both in cases of suspicion and in confirmed cases.



PHOTO: KIM JENSEN, CISU



### 5.7 Reporting of irregularities and suspicion of corruption

Grant holders and their partners are obliged to report any significant irregularities that occur during the implementation of CISU-supported activities. This reporting obligation is set out in grant agreements and in CISU's administrative guidelines.

Reportings are treated seriously and professionally and will not lead to reprisals or discriminatory treatment by CISU. However, if it is demonstrated that false accusations have been made, CISU may take action — for example:

- Disciplinary measures against employees (warning, dismissal or summary dismissal)
- Termination of contractual relations with grant holders or suppliers
- Reporting to the police in criminal cases
- Claims for compensation for any financial loss.

All reports of irregularities and suspected corruption in CISU-funded projects are handled in accordance with the Ministry of Foreign Affairs' guidelines for funding schemes, the grant contracts and cooperation agreements between grant holders and partners.

An anti-corruption clause is mandatory in all contracts:

*"No offer, payment, consideration or benefit of any kind, which could be regarded as an illegal or corrupt practice, shall be made – neither directly nor indirectly – as an inducement or reward in relation to tendering, award of the contract, or execution of the contract. Any such practice will be grounds for the immediate cancellation of this contract and for such additional action, civil and/or criminal, as may be appropriate. At the discretion of the Danish Ministry of*

*Foreign Affairs, a further consequence of any such practice can be the definite exclusion from any tendering for projects, funded by the Danish Ministry of Foreign Affairs."*

#### 5.7.1 How to report irregularities and suspicions of corruption

All grant holders under CISU funding schemes must immediately report to CISU if they discover or have reasonable suspicion of theft, fraud, corruption, misuse or other irregularities.

Reports should be submitted via [the reporting form](#) available on CISU's website.

#### 5.7.2 When to report

Reporting should be immediate and no later than within 14 days, if any of the following occur:

- Significant difficulties arise in delivering the activity, including budget problems
- Serious problems occur with authorities in the partner country, with a partner organisation, or with deployed staff
- There is reasonable suspicion of theft, fraud, corruption or misuse of CISU funds
- There is suspicion of misuse of funds from other donors where the same people in management are involved in a CISU grant
- An internal or external investigation is initiated (e.g. external audit or legal inquiry)
- Significant political risks emerge or there is a risk of damage to the organisation's or CISU's reputation.

#### 5.7.3 Processing reports

CISU reviews all reports and records them in its grant management system. If CISU finds grounds for a reasonable suspicion of fraud, corruption, misuse or other irregularities in connection with a grant financed from CISU's funds (and thus the Ministry of Foreign Affairs), CISU is obliged to forward the report to the Ministry of Foreign Affairs.

Before forwarding, CISU will review the reporting together with the concerned organisation(s). After the review, the Ministry will inform CISU whether the report is forwarded to the Auditor General (Rigsrevisionen) and thereby registered as a C-case (Corruption case). C-cases are described and published on the Ministry's/Danida's website, with information and status updates in accordance with GDPR.

While a case is open, updated reports must be provided every six months (from both the grant holder and CISU) until the case is concluded.

#### 5.7.4 Composition of the reporting group

CISU has established a dedicated reporting group for reviewing reports of irregularities and suspected corruption. The group consists of a grant manager(s) and controller and reports to CISU's management.

The reporting group may call on anyone in CISU to assist in clarifying a case. In exceptional circumstances the group may contract an external expert to ensure the best possible basis for decisions. The general rules on impartiality apply to the group's composition (see section 4.2.2).

#### 5.7.5 Decisions by the reporting group, the Ministry and the Auditor General

On receiving a report, CISU decides whether there is reasonable suspicion or evidence of irregularities and/or corruption. If CISU concludes there are grounds for reasonable suspicion or documented irregularities, it is forwarded to the Ministry of Foreign Affairs.

Only the Ministry of Foreign Affairs and the Auditor General (Rigsrevisionen) may make final decisions in the case, including decisions on case closure and any demands for repayment.

A case may only be closed once it has been satisfactorily clarified and once sufficient and effective measures have been taken that are proportionate to the seriousness of the case. The Ministry will publish ongoing follow-up and status information on its website in cooperation with the Auditor General.

In CISU, we distinguish between two types of reportings related to grants and the organisations or individuals involved in CISU-funded projects

- **Reports:** Used by grant holders and their partners to report irregularities in their own projects or among their partners.
- **Complaints:** Used for cases concerning the behaviour of CISU, grant holders or member organisations.

# 6. Security

## 6.1 General security

### 6.1.1 Legal security

CISU operates in accordance with the legal principles described in Chapter 4 (Legal Principles). All contracts with employees, consultants, suppliers and others are stored securely and fully in compliance with applicable legislation on personal data and accounting.

CISU has an ongoing insurance agreement with Willis Towers Watson covering work-related injuries, business insurance, business travel, and board and professional liability. Regular meetings are held with Willis, and CISU has both a dedicated contact person and access to 24-hour support.

### 6.1.2 Financial security

CISU's bank accounts are administered through a major Danish bank with B and C authorisations, ensuring that no individual has sole access to the accounts.

- Wireless keyboards are not used for online banking to avoid security risks
- All bank accounts are regularly reconciled by the controller
- Bank reconciliations are included in both unannounced and annual audit reviews
- Audit assignments are tendered every 3–5 years, and in the case of longer cooperation, staff rotation is required within the audit firm to ensure independence.

### 6.1.3 Cooperation on staff security

Close cooperation has been established between management and staff concerning occupational health and safety. CISU has an elected health and safety representative who:

- Coordinates workplace assessments (APV)
- Provides assistance in specific occupational health cases
- Participates in cooperation committee meetings with management and

the trade union representative, where workplace assessments are discussed twice a year.

Occupational health and safety are included in both secretariat policies and the physical working environment at the office. CISU's management team also strives to remain available around the clock so that staff can receive support in case of security-related incidents.

### 6.1.4 Physical security

CISU's office in Aarhus is protected by a joint Falck subscription, fire safety systems and alarm systems.

Workplace assessments (APV) ensure compliance with rules on office layout and indoor climate. All workstations are equipped with ergonomic furniture, and specific needs are met on a case-by-case basis within budgetary limits.

### 6.1.5 Communicative security

CISU has an internal IT working group and a contract with an external IT provider responsible for all systems.

To protect data and communication, CISU uses:

- Passwords
- Antivirus programs
- Backup solutions
- Global Secure Access for secure external access

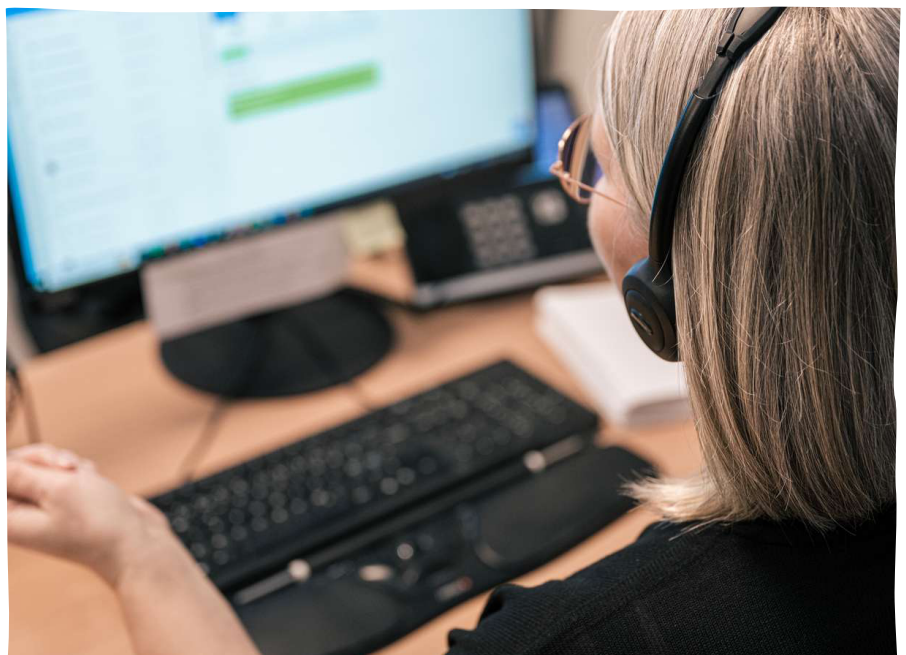
For business travel to high-risk areas, CISU may provide "clean" laptops and mobile phones with local SIM cards to increase data security.

## 6.2 Security on international travel

CISU has developed clear guidelines for security and contingency planning in connection with official international travel for staff. All CISU employees are covered by the organisation's insurance policies. External consultants are themselves responsible for arranging appropriate insurance. Guidelines can be provided upon request.

If there are any questions or doubts about the security of a specific trip, the management team makes the final decision on whether the trip should go ahead.

PHOTO: KIRSTEN ADLER



# 7. Complaints to CISU

## 7.1 Introduction of principles

Everyone has the right to submit a complaint to CISU. Complaints can relate to any of CISU's areas of work, including matters covered by this Code of Conduct.

CISU seeks to promote an open and safe culture, where access to submit complaints is straightforward, the handling process is transparent, and decisions are well-reasoned.

Complaints submitted will never result in reprisals or discriminatory treatment by CISU. However, if false claims are submitted and documented, CISU may take action, which could include:

- Disciplinary measures against staff (warning, dismissal, or summary termination)
- Termination of contracts with grant holders and suppliers
- Reporting to the police in cases involving criminal offences
- Claims for compensation for damages caused

### Types of complaints

Complaints are divided into three main categories:

- **Grant complaints (K1):** Complaints about processing in CISU's grant assessment system
- **Internal complaints (K2):** Complaints about internal matters within CISU, including staff, management, and board members
- **External complaints (K3):** Complaints about grant holders and partners in relation to CISU-funded activities

For complaints of type K2 and K3, the whistleblower scheme may be used (see section 7.5).

In CISU, we distinguish between two types of reportings related to grants and the organisations or individuals involved in CISU-funded projects

- **Reports:** Used by grant holders and their partners to report irregularities in their own projects or among their partners.
- **Complaints:** Used for cases concerning the behaviour of CISU, grant holders or member organisations.

## COMPLAINT HANDLING PROCESSES

All complaint types (K1, K2, and K3) follow the same basic process:

- The complaint is submitted to CISU via the available channels (email or web form)
- CISU's designated complaints officer receives the complaint, confirms receipt, and logs it
- The complaints officer informs management and/or the board about the complaint
- A complaints panel is formed in accordance with the relevant guidelines for the type of complaint
- The complaint is handled confidentially and based on the relevant rules and procedures
- A decision is made, and the relevant parties are informed of the outcome.



### 7.2 Complaints about processing in CISU's grant assessment system (Grant Complaints) [K1]

#### 7.2.1 What does this type of complaint cover?

Applicants to CISU's funding schemes can submit a complaint if they believe formal errors occurred in the processing or in the assessment committee's decision. This concerns cases where procedures or rules were not followed correctly.

A formal error occurs, if:

- One or more of the key legal principles (see section 4.2) were not followed
- Other assessment criteria than those stated in the fund guidelines were applied
- Requirements were imposed on the applicant or application that were not described in the fund guidelines.

It is important to note that it is not possible to complain about a decision simply because one disagrees with the judgement or assessments made by grant managers, grant consultants, or the grant assessment committee. Complaints can only concern formal errors in the processing – not disagreements with the professional assessment itself.

#### 7.2.2 How to submit a complaint

All applicants can submit a K1 complaint through the dedicated online form: [How to Submit a Complaint](#)

The form can be submitted directly online or downloaded and sent to [complaints@cisu.dk](mailto:complaints@cisu.dk).

The complaint must address the following questions:

##### 1. What is the complaint about?

- a. Breach of legal principles – if yes, which ones?
- b. Use of other assessment criteria than those in the guidelines?
- c. Use of invalid requirements for the applicant or application?

##### 2. What outcome is desired from the complaint?

Complaints that do not answer these questions will be rejected.

#### 7.2.3 Complaint deadline

A K1 complaint must be submitted no later than four months after the applicant receives CISU's decision

#### 7.2.4 Composition of the complaints panel

Complaints about processing are handled by a special complaints panel consisting of three people:

- Two members of CISU's board (so that the board always has a majority)
- One representative from CISU's management team

The panel may, when necessary, request assistance from relevant persons within CISU, including a representative from the relevant assessment committee. In special cases, the panel may involve an external expert to ensure the best possible decision-making basis.

General rules on conflicts of interest also apply to panel members (see section 4.2.2).

#### 7.2.5 Panel decisions

The complaints panel decides by simple majority. Possible outcomes include:

##### A. Complaint rejected - for example, if:

- The complaint concerns a matter outside the scope of formal errors
- The complaint is based solely on disagreement with professional judgement
- The complainant is not entitled to complain
- The complaint deadline has passed

**B. Grant assessment committee decision upheld** - if the panel finds no formal errors in processing. Minor formal errors is not taken into account if they would not have affected the outcome; In such cases, the decision may, where appropriate, be accompanied by a formal expression of criticism.

**C. Case referred back for reconsideration** - if the panel finds significant formal errors that may have influenced the outcome. A new and correct processing could result in a different decision.

A complaint cannot result in a decision that leaves the complainant worse off than before. For example, a complaint about a partial grant cannot result in a complete rejection.

The panel's decision is final and cannot be appealed.

The management representative in the panel is also responsible for:

- Informing the grant assessment system if a complaint concerns an application prepared by a member
- Informing the grant assessment system once the decision is made
- Informing the secretariat of the decision and lessons learned
- Ensuring relevant advisors share lessons with the grant assessment system at the following calibration meeting or other joint professional meetings.

#### 7.2.6 Panel response deadline

The K1 complaints panel must conclude the case and inform the complainant no later than four months after CISU receives the complaint in writing.

### 7.3 Complaints about internal matters and/or CISU staff/management/board members [K2]

#### 7.3.1 What does this type of complaint cover?

Anyone can submit a K2 complaint to CISU if there are concerns about the quality of our work or suspected unethical behaviour. This may include dishonesty, harassment, exploitation, abuse, violence, or other actions that go against CISU's values and principles.

#### 7.3.2 How to submit a complaint

Anyone can submit K2 complaints about internal matters or individuals at CISU using the dedicated online form: [How to Submit a Complaint](#)

The form may also be downloaded and sent by email to [complaints@cisu.dk](mailto:complaints@cisu.dk).

It is also possible to report concerns by calling a CISU staff member, management representative, or board member, or by visiting in person for guidance on a specific situation.

The complaint form must answer the following questions:

##### 1. What is the complaint about?

- Breach of safeguarding principles – if so, which; harassment, exploitation, abuse, etc.?
- Who is the complaint about; staff, management representative, board member, etc.?
- Describe the situation, including place, time, and actions

##### 2. What outcome is desired from the complaint?

Complaints that do not address these questions will be rejected.

#### 7.3.3 Complaint deadline

CISU aims for fair and timely handling of K2 complaints:

- Complaints should be submitted as soon as possible
- Complaints must be submitted no later than four months after becoming aware of the incident or when the incident occurred.

#### 7.3.4 Composition of the complaints panel

Panels handling complaints about CISU staff or internal matters are comprised depending on who the complaint concerns:

- If the complaint concerns a staff member:** chairperson, deputy chairperson, and a management representative. The Trade Union representative or other staff member may participate as agreed with the complainant.
- If the complaint concerns a management member:** Chairperson, a management representative not involved in the complaint, and the internal auditor. If the entire management team is involved, the panel consists of chairperson, deputy chairperson, and the internal auditor.
- If the complaint concerns a board member:** chairperson, deputy chair, and the internal auditor. If necessary, an external expert with relevant skills may be included. If the chairperson or deputy chairperson are involved in the complaint, they are replaced by the internal auditor and an external expert appointed by the internal auditor. If the entire board is involved, the panel consists of the internal auditor, an external expert appointed by the internal auditor, and a management representative.

The panel may request information from anyone at CISU to clarify the case. In exceptional cases, an external expert may be contracted.

General rules on conflicts of interest apply (see section 4.2.2).

#### 7.3.5 Panel decisions

The complainant and any other relevant parties will be informed of the outcome. The Ministry of Foreign Affairs will be informed if the case affects CISU's agreements with the Ministry.

Possible outcomes:

**A. Rejection** with explanation to the complainant

**B. Uphold complaint, refer for internal handling** in the secretariat if legitimate but outside the complaints system's mandate (e.g. HR or employment-related complaints)

**C. Uphold complaint, refer to another authority** (e.g. police) if legitimate but outside the complaints system's mandate (e.g. criminal matters)

The panel's decision is final and cannot be appealed.

#### 7.3.6 Panel response deadline

CISU aims for fair and conscientious handling of K2 complaints:

- A panel must be appointed, and the complaint process begun, within two months
- Completion time depends on the complexity of the case
- CISU always seeks an efficient and fair process under the circumstances.

### 7.4 Complaints about grant holders and partners in CISU-funded activities [K3]

#### 7.4.1 What does this type of complaint cover?

Anyone may submit a complaint to CISU about grant holders or partners if there are suspicions of potential violations such as harassment, exploitation, abuse, violence, or other unethical conduct within CISU-supported activities.

Complaints should generally be raised and handled as close to the incident as possible. For example, complaints from the target group should normally be directed to the local partner. If the partner is the cause of the complaint, it should be escalated to the next level, usually the Danish organisation/grant holder. There may be multiple levels in the chain.

CISU receives and handles all complaints concerning the Danish organisation/grant holder and may, in special cases, handle complaints from target groups, local partners, or other relevant actors, in line with standards such as the *Core Humanitarian Standards (CHS)*.

#### 7.4.2 How to submit a complaint

Anyone can submit K3 complaints about grant holders or local partners using the dedicated online form: [How to Submit a Complaint](#)

The form may also be downloaded and sent by email to [complaints@cisu.dk](mailto:complaints@cisu.dk).

It is also possible to report concerns by phone or in person for guidance on a specific situation.

The complaint form must answer:

##### 1. What is the complaint about?

- a. Breach of safeguarding principles – if yes, which; harassment, exploitation, abuse, etc.
- b. Breach of anti-corruption, legal, or ethical principles – if yes, which; misuse of funds, law violations, etc.
- c. Who is the complaint about; recipient/partner board, management, staff, etc.?
- d. Describe the situation with place, time, and actions.

##### 2. What outcome is desired from the complaint?

Complaints not addressing these questions will be rejected.

#### 7.4.3 Complaint deadline

CISU aims for fair and timely handling of K3 complaints:

- Complaints should be submitted as soon as possible
- Complaints must be submitted no later than six months after becoming aware of the incident or when the incident occurred.

#### 7.4.4 Composition of the complaints panel

Panels handling complaints related to implementation of CISU-funded activities must have at least three members: one board member and two representatives from the management team. Panels may be supplemented with relevant secretariat staff. Board representation follows a rotation principle.

The panel may request information from anyone within CISU or, in exceptional cases, contract an external expert to ensure the best decision-making basis.

Conflict of interest rules apply (see section 4.2.2).

#### 7.4.5 Panel decisions

There are four possible outcomes. The complainant and any other relevant parties will be informed. The Ministry of Foreign Affairs will be informed if relevant.

**A. Rejection** with explanation

**B. Uphold complaint, refer to recipient/partner** for handling

**C. Uphold complaint, refer to secretariat** if legitimate but outside the complaints system's mandate (e.g., HR-related matters)

**D. Uphold complaint, refer to another authority** (e.g. police) if legitimate but outside the complaints system's mandate (e.g. criminal matters)

The panel's decision is final and cannot be appealed.

#### 7.4.6 Panel response deadline

CISU aims for responsible and conscientious handling of K3 complaints:

- A panel must be appointed, and handling begun, within two months
- Completion time depends on the complexity of the case
- CISU always seeks an efficient and fair process under the circumstances.



### 7.5 Whistleblower Scheme

#### 7.5.1 Definitions and basis

CISU uses Transparency International's definition of whistleblowing:"

*"The disclosure of information about a perceived wrongdoing in an organisation, or the risk thereof, to individuals or entities believed to be able to effect action."*

This includes reporting illegal or questionable matters related to CISU-funded activities and/or CISU staff. The scheme is based on Danish law and EU rules and aims to allow serious concerns to be raised safely. All cases are handled objectively, factually, and respectfully.

The whistleblower scheme may be used for:

- **Internal complaints (K2):** Complaints about internal matters within CISU, including staff, management, and board members
- **External complaints (K3):** Complaints about grant holders and partners in relation to CISU-funded activities

The scheme does not apply to Grant complaints (K1): Complaints about processing in CISU's grant assessment system.

#### 7.5.2 How to report via the Whistleblower scheme?

Anyone may use the dedicated online form for K2 and K3 complaints: [How to Submit a Complaint](#) - indicating that the complaint is under the whistleblower scheme.

CISU recognises that whistleblowers may face significant pressure. CISU will make it as easy as possible for whistleblowers to inform CISU, while protecting them from reprisals from the organisation or persons they are reporting on – including employers or others they otherwise depend on.

Whistleblower identities are protected, and reports may be made anonymously. Reporting concerns is always a safe option and will not lead to sanctions even if the information turns out to be incorrect.

However, documented false claims may result in actions such as disciplinary measures against members of staff, contract termination for grant holders and suppliers, police reporting in criminal matters or claims for damages.

#### 7.5.3. Rights of reported individuals

The whistleblower scheme ensures safe and confidential reporting of serious concerns, but it is equally important that any persons mentioned in reports are treated fairly and with respect.

Individuals mentioned in a report have the following rights under Danish and EU whistleblower laws:

**Confidentiality:** All information, including the identity of the person involved, is treated confidentially. Only relevant persons for handling a report have access to information

**Information:** Where possible, the person will be informed that a report has been made and its content - as soon as possible so as to not affect the investigation

**Right to Respond:** Before a decision is made, the person can give their version of events. This is important for fair and balanced processing

**Protection from unjust consequences:** Groundless or incorrect reports will not result in negative consequences. The case will be closed confidentially, discreetly and respectfully.

#### 7.5.4 Reporting deadlines

Reportings should be made as soon as possible after the incident or after the whistleblower becomes aware of it.

#### 7.5.5 Handling process

Reports are assessed by CISU's management and chairperson, who decide whether to follow the processes described in sections 7.3 or 7.4, depending on the complaint type.



PHOTO: KIRSTEN ADLER

# 8. Anti-terror

## 8.1 Introduction

The Danish Ministry of Foreign Affairs requires the implementation of an anti-terror clause in all funding schemes, including CISU's. The anti-terror clause reflects an obligation to prevent any connection to terrorism and to comply with international sanctions. It underlines the seriousness of such matters, as breaches of these obligations may lead to termination of agreements and repayment of funds.

### *CISU's requirements for grant holders and local partners:*

- According to CISU's funding guidelines, it is the responsibility of the Danish organisation to screen local partners and others receiving grant funds to ensure they are not listed on the EU and UN terrorism lists. When selecting partners, screening must be carried out against the EU and UN lists.
- CISU includes the Ministry of Foreign Affairs' anti-terror clause in all grant contracts between CISU and the Danish organisation.
- CISU also requires that the anti-terror clause is included in all cooperation agreements between the Danish organisation and partners in the partner country. This requirement is also described in CISU's grant management guidelines for the various funds administered by CISU.
- CISU disburses grant funds to the Danish grant holder upon request. The Danish grant holder is responsible for disbursing funds to local partners.

## 8.2 CISU's requirements and monitoring

The requirement for ongoing monitoring is set out in the grant letter sent with the contract to all grant holders. The letter refers to CISU's monitoring tools, which include screening in relation to the anti-terror clause.

When monitoring Danish organisations and local partners, CISU always checks that all of the Ministry of Foreign Affairs' clauses are included in cooperation agreements.

CISU actively conducts monitoring visits with a selection of grant holders, both in Denmark and with their local partners. The monitoring includes, among other things:

- Use of monitoring checklists covering both financial monitoring and assessment of the organisations' compliance with their contracts with CISU (accountability compliance)
- Verification that partnership agreements include the anti-terrorism clause
- Assessment of the organisations' procedures to ensure that they do not cooperate with parties listed on EU or UN sanctions lists
- Spot checks and assessment of local partners' financial systems and capacity
- Collection of documentation or reports from the Danish organisations' ongoing monitoring of their local partners.

CISU uses its own checklists during monitoring visits and encourages Danish organisations (grant holders) to use the same tools in their ongoing cooperation with partners. The checklists and other management resources are available on CISU's website.

All monitoring activities are documented in a monitoring report.

## 8.3 CISU's anti-terror initiatives and capacity building

To support member organisations and grant holders' anti-terror work, CISU has developed a number of resources:

**Accountability Learning Site:** includes a specific page on anti-terror, with good practice examples, standards, and relevant links: [Anti-terror learning site](#)

**Course activities:** CISU offers training with several courses that strengthen the capacity of Danish grant holders and local partners to manage grants responsibly. Under the course category "Organisation & Management" there are courses such as grant management, financial management, project monitoring visits and accountability - including the use of checklists for monitoring. The current list of available courses can always be found on [CISU's website](#).

## 8.4 CISU's anti-terror screening

CISU screens contracted partners, co-operation partners, suppliers, and others against the EU and UN terrorism lists using the following regularly updated links:

- **EU Sanctions List:** [Consolidated list of persons, groups and entities subject to EU financial sanctions](#)
- **UN Sanctions List:** [UN Security Council Consolidated List](#)

CISU – Civil Society in Development  
Klosterport 4x, 3. sal | 8000 Aarhus C | Tel: +45 86 12 03 42  
Alle hverdage 10-15 | [cisu@cisu.dk](mailto:cisu@cisu.dk) | [www.cisu.dk](http://www.cisu.dk)

