

GUIDES TO GOOD GOVERN- ANCE

No. 10

Guide on Whistleblowing in the Defence and Security Sector



CENTRE FOR INTEGRITY
IN THE DEFENCE SECTOR



Norwegian Ministry
of Defence

CENTRE FOR INTEGRITY IN THE DEFENCE SECTOR

The Centre for Integrity in the Defence Sector (CIDS) promotes integrity, anti-corruption measures and good governance in the defence sector. Working with Norwegian and international partners, the centre seeks to build competence, raise awareness and provide practical means to reduce risks of corruption through improving institutions and education and training. CIDS was established in 2012 by the Norwegian Ministry of Defence (MOD) and was officially appointed as NATO's Department Head in the new discipline area, established through the Building Integrity Programme in 2013. The Centre is now an integral part of the MOD.

CONTENTS

INTRODUCTION	2
1. TERMS	4
2. FREEDOM OF EXPRESSION.....	6
3. STAGES OF A WHISTLEBLOWING CASE.....	7
4. WHISTLEBLOWING.....	8
5. RECEIPT OF REPORT OF WRONGDOING.....	10
6. PRELIMINARY INVESTIGATIONS	12
7. IMPLEMENTATION AND FEEDBACK	14
8. FOLLOW-UP	16
9. DATA PROTECTION.....	17
10. EXAMPLES OF WHISTLEBLOWING CASES.....	19

Introduction

The Guide on whistleblowing in the defence and security sector contains practical advice and measures for those receiving or dealing with a report of wrongdoing, based on how cases of Whistleblowing are handled in the Norwegian Defence Sector. The Guide has been developed based on procedures and experiences from different agencies in this sector.

The Guide is intended to:

- Increase general awareness about whistleblowing and different whistleblowing situations.
- Enable managers and others who receive reports of wrongdoing to deal with this in a proper manner.
- Identify and prevent wrongdoing in the sector.

Defence personnel (including enlisted personnel), external employees, contract staff, craftsmen, external persons and other parties with no affiliation with the agency in question have the right to report wrongdoing in the defence sector.

Person's reporting wrongdoing can themselves decide who to notify, whether they notify a person or one of the control units. This means that everyone in the defence sector may receive a disclosure of wrongdoing at some point and must be prepared to deal with it or, if appropriate, pass the case on to the relevant authority.

Whistleblowing has greatest value when the disclosure is handled thoroughly, the whistleblower is protected, procedures are initiated to clarify whether wrongdoing exists, and the wrongdoing ceases.

This Guide has been written by the Internal Auditor Unit of Norwegian Defence. Several of CIDS' international experts have contributed. I would like to thank everybody who has given a hand, including the CIDS Editor, Mr. Hans Myhrengen.

The Guide has been devised using the Norwegian Defence sector's guidelines for whistleblowing. We would also underline that the document reflects the legal Norwegian framework, as being a member of the European Economic Area (EEA). In light of this, the legal framework of the European Union on a number of issues covered in the Guide also applies in Norway.

CIDS is happy to receive feedback to the guide.

Oslo, 2 November 2020



Per Christensen

Director

1. Terms

Term

Reporting wrongdoing

Reporting wrongdoing (whistleblowing) entails sounding the alarm about a situation or reporting an issue of concern you have become aware of within the defence sector.

Reporting issues of concern at the workplace in Norway is regulated by the Working Environment Act. In the Act, such a disclosure is not defined, but the Act states the following: 'An employee has a right to report wrongdoing at the employer's undertaking.'

When an employee becomes aware that wrongdoing exists or has existed, the provisions of the Working Environment Act will apply, and the employee will be protected against unfavourable treatment as a result of the disclosure, provided that the correct procedures have been followed.

Wrongdoing

Wrongdoing, referred to as 'censurable conditions' in Norwegian legislation, includes violations of statutory Acts and internal guidelines, criminal offences and breaches of other statutory orders or prohibitions, contraventions of the defence sector's ethical guidelines as well as breaches of general ethical standards that have widespread support in society.

Retaliation

Retaliation is any kind of unfavourable treatment that can be seen as a consequence of and reaction to whistleblowing. Retaliation is prohibited.

The prohibition also applies to formal sanctions such as dismissal with notice, suspension and summary dismissal, in addition to sanctions such as changes to work tasks and internal transfers.

A whistleblower

A whistleblower is someone who speaks up about wrongdoing in the defence sector.

Subject of the whistleblowing

The term 'subject of the whistleblowing' is used to refer to the person or persons identified as the alleged person responsible for the reported wrongdoing.

Internal whistleblowing	Internal whistleblowing is when the whistleblower raises issues of concern internally in the defence sector. For example, informing colleagues, employee representatives or a management representative.
External whistleblowing	<p>External whistleblowing is when the whistleblower provides information and documents to persons or organisations outside the defence sector, for example supervisory authorities, professional forums and the media etc.</p> <p>In Norway, The Internal Auditor Unit of the Ministry of Defence is the external whistleblowing channel for the agencies in the Defence Sector. In addition, the agencies in the sector have their own internal channels.</p>
Recipient of the disclosure	The recipient of the disclosure is the person receiving the disclosure, for example, a colleague, the immediate manager, the control unit, the employee representative, the safety officer, board member etc.
Executive officer	The executive officer is the person who deals with the disclosure. He/she may be the person to whom the wrongdoing is reported or someone who becomes involved with the case at a later stage.
Whistleblowing case	The term 'whistleblowing case' is used to refer to a case in relation to the whistleblower and the wrongdoing as well as the case as a whole.
HR case	An HR case is any case related to the employee's working conditions, for example problems cooperating, refusal to obey orders or lack of competence. It can be challenging to distinguish between a whistleblowing case and an HR case. The control unit should be consulted if there is doubt.
Whistleblower protection/ Whistleblower status	<p>Whistleblower protection is the protection offered to the whistleblower by the employer. It entails protection against retaliation.</p> <p>Whistleblower is the status given to the person who reported wrongdoing, and who consequently should not be subject to retaliation.</p>
Anonymous disclosure	Anonymous disclosure refers to situations where the recipient of the disclosure does not know the identity of the whistleblower. For example, this might refer to an unsigned letter or other anonymous communication.
Confidential disclosure	Confidential disclosure refers to situations where the recipient of the disclosure knows the identity of the whistleblower but keeps this confidential. Confidentiality means that the executive officer must ensure that information and information systems are only accessible to authorised parties.
Contradiction	Contradiction means that the person(s) alleged to be responsible for the wrongdoing has the right to be heard and to give their version before the case is concluded.
Impartiality	In a whistleblowing case, the person who deals with the disclosure must be impartial. The person must always be able to make decisions in the whistleblowing case neutrally, based on objective criteria. If the person is not impartial, for instance because of close family bonds to the whistleblower, this means that trust in him/her may be weakened. If such circumstances exist, the rules on impartiality state that the person shall not participate in the processing of the specific case or the decision made in the case.

2. Freedom of expression

Freedom of expression is the right everyone has to speak freely their minds about anything they wish to, regardless of content, time, form and medium within the reasonable boundaries fixed by the law. This means, for example, that everyone has the right to write a contribution to the newspaper or make a comment on social media, but not to make false and harmful claims or statements against the law.

Reporting wrongdoing at the workplace is a special form of utterance, and if this is reported in line with the sector's guidelines on whistleblowing, the whistleblower will be protected against unfavourable actions following the disclosure (prohibition against retaliation).

The defence sector should be a transparent organisation characterised by a robust culture of free expression, supported by the Rule of Law. Staff are encouraged to participate in creating the public discourse. It is possible to report concerns via the whistleblowing scheme. According to Norwegian law, all employees have the right to express their critical opinions with regard to their own workplace.

This principle is also laid out in Article 11.1 of the EU Charter of Fundamental Rights: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."

There must be transparency regarding norms and values, discussion on how internal criticism should be evaluated, and talks and meetings about a robust culture of free expression. Moreover, information must be provided about whistleblowing and the defence sector's guidelines on whistleblowing. There must be a leadership focus on transparency, as well as interaction and cooperation with internal health and safety services and employee representatives.

By means of good whistleblowing procedures and a transparent culture of free expression, the defence sector should – as far as possible – make every effort to ensure an open organisation.

3. Stages of a whistleblowing case

Sound procedures for dealing with a disclosure of wrongdoing are of overarching importance for all stages of a whistleblowing case. The various stages will often overlap, and the recipient of the disclosure must therefore be aware that the elements in the different stages may need to be dealt with simultaneously.

Chapters 5–9 describe how to deal with a whistleblowing case. The chapters are divided in accordance with the various stages shown in the figure.

The colours used in the figure illustrate that while different people are responsible for reporting wrongdoing, receipt of disclosure and follow-up, the preliminary investigations, implementation and feedback are normally carried out by the same executive officer.

The broken line illustrates how the whistleblowing process ends in experiential feedback learning and continual improvement of whistleblowing procedures and transparency culture.

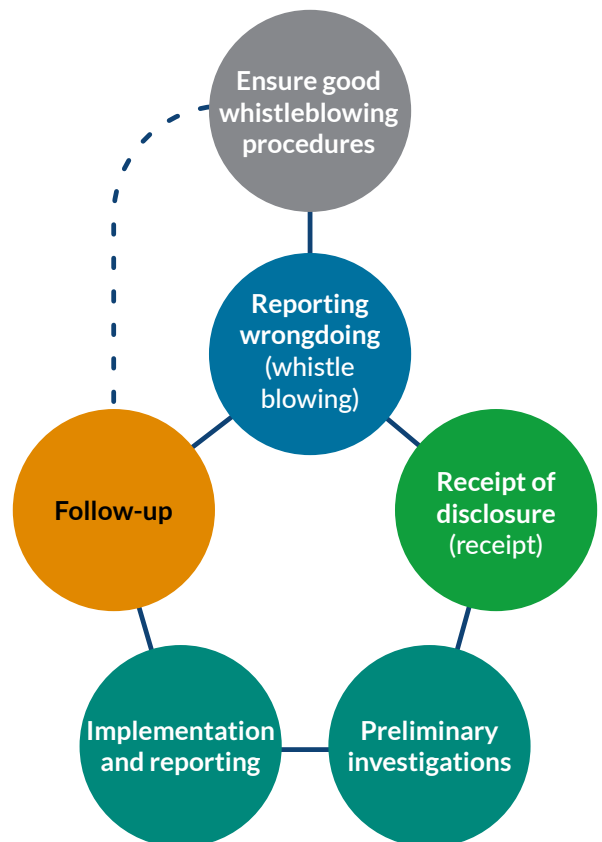


Figure 1: The whistleblowing process

4. Whistleblowing

Due to the often delicate matter of reporting possible wrongdoings, those who reports wrongdoing may themselves choose whom to report to. This means that everyone must be prepared to receive a disclosure of wrongdoing. Sometimes it may be challenging to recognise that you have received a whistleblowing disclosure, as opposed to this being a situation where someone wants to air an opinion or give feedback about an issue of concern. If you are uncertain whether you have received a disclosure of wrongdoing, you should clarify whether the person concerned is officially reporting wrongdoing or letting you know informally about an issue of concern. It is also possible to contact the control unit in the organisation if you are unsure whether someone has reported wrongdoing. In the defence sector, there are no formal requirements regarding how to report wrongdoing. The recipient of the disclosure must be aware that reports of whistleblowing can take several forms.

4.1 WRONGDOING

The specific rules that apply to whistleblowing only come into play when 'wrongdoing' is

reported in the defence sector. The person receiving such a disclosure must therefore assess whether the issue of concern reported is deemed to be wrongdoing. Examples may be issues of concern that are, or might be, in conflict with laws and regulations. Issues of concern that conflict with the general opinion of what is justifiable or ethically acceptable are also deemed to be wrongdoing. Issues of concern that do not fall into this category might be HRM matters¹, political utterances, cooperation problems or professional disagreements.

4.2 RESPONSIBLE WHISTLEBLOWING

An employee can always report wrongdoing internally, or externally to a public supervisory authority. An employee could also notify the media or the general public externally, according to specified condition. Example: Reporting wrongdoing in line with the defence sector's whistleblowing procedures is always permitted. However, if the whistleblower has reported wrongdoing publicly, for example to the media, more stringent requirements for justifiability may need to be imposed.

¹ HRM: «Human Resource Management».

4.3 PROHIBITION AGAINST RETALIATION

Any unfavourable reaction that can be seen as a consequence of and a reaction to whistleblowing shall, in principle, be regarded as retaliation. Retaliation must be prohibited by law, and it is vital that the person who receives and processes the disclosure keeps this in mind. In some situations, measures to prevent retaliation may be necessary, and if the situation so indicates, HSE² support and other follow-up may be considered.

4.4 GENERAL

Below is a list containing general advice on dealing with whistleblowing cases:

- All disclosures must be taken seriously and treated as whistleblowing, including anonymous disclosures.
- The choice of whistleblowing method shall have no significance for how the case is dealt with. All cases should be handled in accordance with the regulations.
- All disclosures must be dealt with without unwarranted delay.
- If the disclosure applies to one or more persons, the person(s) in question must be allowed to comment on information that applies to themselves.
- The recipient of the disclosure must safeguard confidentiality and ensure that the fewest possible number of people are involved.
- It must be decided at an early stage, and on an ongoing basis, whether it is necessary to inform the management and implement risk-based measures.
- The recipient of the disclosure must protect all persons involved.
- The focus must be on the alleged wrongdoing, and not the person.
- The subject of the whistleblowing is innocent until proven otherwise.
- The recipient of the disclosure must be familiar with or familiarise him/herself with the defence sector's guidelines on whistleblowing.
- The executive officer must ensure that documentation is stored securely and in accordance with the defence sector's guidelines.
- The executive officer must be aware of the risk of retaliation.

2 HSE: «Health, Security, Environment».

5. Receipt of report of wrongdoing

5.1 RECIPIENT OF THE DISCLOSURE AND THE EXECUTIVE OFFICER

The person receiving a report of wrongdoing is defined as the recipient. The recipient of the report must carry out a preliminary assessment to decide whether he/she should function as the executive officer or whether the case should be transferred to, for example, a manager, a functional unit or another control unit. The recipient of the report must assess, among other things, whether he/she is qualified to deal with the disclosure, keeping in mind their own authority, competence and impartiality. In the following, the person dealing with the report is termed as the executive officer, regardless of level. In many cases, the recipient of the report will also function as the executive officer.

Receipt of a report of wrongdoing triggers a number of requirements, including dealing with the report within reasonable time and in accordance with rules and regulations.

5.2 IS IT A REPORT OF WRONGDOING?

Before initiating a whistleblowing case, the executive officer must first consider whether the issue reported can be defined as wrongdoing

(see chapter 2 Terms and chapter 5.1 for an explanation of 'wrongdoing').

This means that if a person reports an issue that is clearly not 'wrongdoing', the case is not treated under the whistleblowing rules. If in doubt as to whether 'wrongdoing' has been reported, further investigation should take place.

5.3 IMPARTIALITY

A person can be deemed to be lacking impartiality if circumstances exist that can undermine confidence in the person dealing with the case. If such circumstances exist, the rules on impartiality state that he/she must not participate in the processing of the relevant case or in the decision reached.

5.4 COMPETENCE

A person must have sufficient competence to deal with the report of wrongdoing. He/she must have or be given authority to initiate investigations. If complex or serious issues of concern are reported, the control unit must be contacted for guidance.

If the recipient of the report is not competent to deal with it or is not impartial, he/she

must ask the whistleblower for permission to pass the report on to someone who can deal with it. In cases of doubt and when reports are anonymous, the whistleblower channel should be contacted for guidance.

5.5 INFORMATION TO THE WHISTLEBLOWER

The recipient of the report shall give the whistleblower feedback as soon as possible. The whistleblower should be given information about the process, how long it might take and what feedback he/she can expect to receive. Note that the whistleblower is not necessarily a party to the case, and therefore will not normally have the right to full access to case information.

5.6 DOCUMENT PROCESSING

The executive officer must register the report of wrongdoing as a document that must be filed in accordance with the agency's filing routines and the Archives Act and regulations. This means that receipt of the report, case processing and other decisions are documented and stored securely, and that paper documents are locked away while confidentiality rules observed.

The electronic journal must be designed so that it does not reveal information that is subject to the duty of confidentiality or sensitive information available on the internet, including information that can identify the whistleblow-

er. The executive officer must keep a log of relevant information, in accordance with the procedure for receipt and processing of reports of wrongdoing.

5.7 INFORMATION TO MANAGEMENT

The executive officer must decide which level of management should be informed. If the disclosure entails a grave suspicion of wrongdoing, or the case is otherwise of a serious nature, the executive officer must inform the top management. The executive officer must emphasise the potential for harming the agency and/or individuals in the assessment of whether the disclosure entails grave suspicion of wrongdoing. As regards the protection of affected parties on receipt of the report, see chapter 7.4.

5.8 SENSITIVE INFORMATION

A report of wrongdoing may contain sensitive information pursuant to the Security Act. In the case of sensitive information, the information must be dealt with in compliance with the Security Act, and the executive officer must have appropriate security clearance and authorisation.

If the whistleblowing case reveals issues of concern that can affect the security clearance of defence personnel, this must be reported to the immediate manager, the head of security, the head of the agency or the person authorised by the head of the agency.

6. Preliminary investigations

The executive officer must ensure that the report of wrongdoing is dealt with in a thorough and objective manner, with the aim of rectifying the issue of concern that triggered the disclosure.

6.1 PRELIMINARY INVESTIGATIONS

The executive officer should initiate preliminary investigations in order to assess whether the report on wrongdoing is trustworthy. Preliminary investigations can include obtaining written documentation, for example time sheets or electronic material stored in a shared area. If there is a need to secure electronic and physical data, this must be authorised by the appropriate instance in the agency, and must, if relevant, be carried out by competent personnel. In order to map the elements of the case, the executive officer will also be able to conduct physical checks as well as having conversations with people who may know something. It is important that the executive officer treads cautiously at the investigative stage, since an inappropriate approach might have considerable implications for the further processing of the whistleblowing case.

The purpose of conducting preliminary investigations is to map the elements of the case. In

this connection, the executive officer must be aware that if serious wrongdoing is suspected, the top management must be informed. If the executive officer is in doubt as to whether a serious wrongdoing has been reported, he/she must consult the control unit about the course of action.

6.2 THE WHISTLEBLOWER'S PROTECTION AGAINST RETALIATION

The executive officer must assess whether there is a risk of the whistleblower being exposed to retaliation. If there is a danger of retaliation, the employer must implement measures to prevent this. For example, the risk of retaliation will increase if the whistleblower's identity becomes known to more people than necessary.

6.3 THE INTERESTS OF AFFECTED PARTIES

It is important that the whistleblower, the subject of the whistleblowing and other persons involved are properly protected at all stages. A whistleblower is in a vulnerable situation, and the executive officer must be aware of the burden represented by reporting wrongdoing. The whistleblower and the subject of the whistleblowing must be informed that the occupa-

tional health service unit can provide support if required and give information about others who can provide support in whistleblowing cases, such as trade unions or equivalent.

To protect the parties involved, the executive officer must also ensure that the whistleblowing case is dealt with confidentially, and that as few people as possible are informed of the case.

6.4 INFORMATION TO THE SUBJECT OF THE WHISTLEBLOWING

As a main rule, the subject of the whistleblowing must be informed as early as possible that a report of wrongdoing related to him/her has been received, and the anticipated progress of

the case. However, it is important to note that the whistleblower's identity must not be made known to the subject of the whistleblowing. The executive officer must be aware that exceptions may apply in relation to the further processing of the case.

6.5 MEASURES TAKEN DURING THE PROCESSING OF THE CASE

Depending on the type of case, it may be necessary to initiate measures during the processing of the case. Such measures may include securing a dangerous device that is a threat to life or health or shielding information that is of relevance to the case. The control unit can be consulted in cases of doubt.

7. Implementation and feedback

After completion of the preliminary investigations, the executive officer must assess whether wrongdoing has taken place.

He/she must ensure that the case has been clarified to the greatest extent possible. Normally, further investigations must be carried out, for example conversations with other persons who may have some knowledge of the elements of the case, evaluation of documents, registers, time sheets, logs and physical investigations.

The objective of the executive officer is to conclude at the earliest possible stage whether wrongdoing has been reported.

7.1 CONVERSATIONS

In order to map the elements of the case, it may be necessary to have a dialogue with persons involved. The executive officer must ensure that conversational partners receive good information beforehand, and in particular be informed of their right to be accompanied by an independent and trusted third party.

The executive officer should bring a deputy executive officer to take part in the dialogue, and the minutes taken must be verified by the person concerned.

7.2 CONTRADICTION

During the case processing, and before the executive officer decides whether wrongdoing has taken place, the whistleblower, the subject of the whistleblowing and other affected parties must be given the opportunity to present their views on issues of concern that involve them. At the same time, the executive officer must keep in mind that the identity of the whistleblower must not be revealed to more people than strictly necessary.

7.3 FINAL REPORT

The executive officer must prepare a final report, also in cases where the allegation of wrongdoing is found to be without foundation. The final report must describe the content of the disclosure, case processing, conclusion and recommendations.

The executive officer must submit the final report along with the completed disclosure form for reporting wrongdoing and the completed disclosure record.

The executive officer must ensure that the relevant manager, or the person authorised, approves the final report. Normally, this will take place at a principal level.

Following approval, the executive officer must send the final report to the control unit. The control unit must have a complete overview of whistleblowing reports in the agency and the status of measures taken.

7.4 INFORMING THE PARTIES INVOLVED

When the whistleblowing case is concluded, the whistleblower must be informed of the end result. Providing the whistleblower with information during the process, will help reassure him/her that the case is being dealt with in a serious manner, and that speaking up is beneficial. If the whistleblower is anonymous, information cannot be given, and the executive officer must not attempt to discover the identity of the whistleblower.

As a main rule, the subject of the whistleblowing must also be informed of the outcome of the case. It is important that the executive officer shows consideration for this person.

8. Follow-up

8.1 SOLUTION

If it is concluded that wrongdoing has taken place, the recipient of the final report must assess the need for measures and follow-up with regard to individuals and systems. Moreover, it must be decided who will implement measures.

Examples of measures are:

- training
- changes to rules and/or procedures
- initiating an HRM case
- a warning or official reprimand
- assessment of security clearance and authorisation
- formal complaint

It is vital that shortfalls revealed are followed up by measures to prevent similar events in the future.

It is important to protect all parties in the case, and to maintain a focus on preventing retaliation.

8.2 EXPERIENTIAL LEARNING

After the report of wrongdoing has been dealt with, the process must be examined in order to evaluate the processing of the report.

A review of the whistleblowing case is useful, because it will help to improve conditions in the defence sector and whistleblowing procedures.

9. Data protection

9.1 INTRODUCTION

In most cases of whistleblowing, the executive officer will gain knowledge of personal data. The personal data can be linked to the whistleblower, the subject of the whistleblowing or other individuals. The person who receives and processes a report of wrongdoing must comply with the regulations on personal data. Below, the key aspects that apply in a whistleblowing case is described.

The whistleblower, the subject of the whistleblowing and other individuals will hereinafter be referred to as the 'data subject'.

9.2 CONSIDERATION FOR THE WHISTLEBLOWER

The person who receives a report of wrongdoing must ensure that the whistleblower's identity is not revealed to more people than absolutely necessary in relation to the further case processing. The whistleblower should be informed that if the whistleblowing case results in a court case, there may be a legal requirement to inform the court of the whistleblower's name.

9.3 THE RIGHTS OF THE DATA SUBJECT

9.3.1 RIGHT TO INFORMATION

The data subject must be given information about how the agency deals with personal data on him/her. This means that the data subject has the right to know what personal data has been obtained and how it has been used. The data subject has the right to information at the earliest possible stage and at the latest a month after information about the person in question has been obtained.

9.3.2 RIGHT OF ACCESS

If the data subject or others request access, as a main rule they have a right to access all personal data about them that is under processing in connection with the whistleblowing case.

Nevertheless, in practice, access cannot be given to information about the whistleblower's identity or information that can reveal his/her identity, but there are exceptions. The person processing the disclosure has a particular responsibility for protecting the rights of the whistleblower.

9.3.3 EXCEPTION FROM THE RIGHT TO INFORMATION AND THE RIGHT OF ACCESS

If there are grounds for making exceptions from the right to information and the right of access, this can be done following a specific assessment in each individual case. In Chapter 11, some examples of cases in Norway are mentioned where exceptions to the data subject's right to information and right of access may apply. In cases of doubt, the control unit was contacted for guidance.

If there is a considerable risk that providing information may jeopardise the case, the executive officer can decide not to give information or right of access to the data subject. Another example is a situation where respect for the clear and fundamental interests of others indicates that the data subject shall not be given a right to information or right of access.

In order to ensure proper internal decision-making processes, data subjects may also be denied the right to information and right of access once the case processing is underway.

Exceptions shall normally not apply longer than what is necessary and appropriate in the specific case.

9.4 DATA SECURITY

In order to safeguard the security of personal data, all information obtained in connection with the whistleblowing case is stored in a separate folder in the National restricted network, or if necessary, locked in a secure cabinet.

9.5 DELETION OF DATA

As a rule, personal data must be deleted when no longer needed for the purpose for which it was obtained. This means that following the conclusion of a whistleblowing case, as a rule it should no longer be necessary to store the personal data. However, the recipient of the disclosure must be aware that there are several exceptions that may apply.

10. Examples of whistleblowing cases

10.1 CASE 1: ABUSE OF POWER IN THE ARMY

Julie is doing her military service and is over halfway through basic training. During physical training, she has noticed that several recruits are being discriminated against. For example, Sergeant Johansen ordered Julie, two other girls and Christian to run two extra laps. Julie tries to keep out of Johansen's way, partly because he often takes his irritation and anger out on those who are presumably the physically weakest in the group. She has heard him say several times that 'girls are born with a poorer physique and have to be pushed harder during basic training – and the same applies to boys who've spent their entire adolescence playing computer games'.

Julie did not think that such attitudes still existed in the armed forces, especially after the introduction of compulsory military service for women. She therefore decides to raise the issue with Staff Sergeant Hagen. Julie's view of Sergeant Johansen is that he is unable to handle his position of power in an acceptable way.

One afternoon, Julie seeks out Staff Sergeant Hagen and explains the situation.

Staff Sergeant Hagen has been in the armed forces for many years and thinks that young

people today are unable to tolerate anything. He dismisses the whole situation and asks Julie to tackle Sergeant Johansen in a different way.

Julie was very surprised by Staff Sergeant Hagen's answer and was uncertain how to pursue the case. If all her superiors reacted in the same way, she would never be heard. She remembered that she had heard about a staff sergeant who was in charge of another group of recruits, who she believed was more open to different views and perspectives.

Julie therefore arranged to meet Warrant Officer (WO) Pedersen, who found that this was a case he had to take further.

10.1.1 HAGEN'S ACTIONS

- Staff Sergeant Hagen did not handle the case in a satisfactory manner. He did not take Julie's concern seriously.
- Julie was clear in her communication with Staff Sergeant Hagen. She told him that Sergeant Johansen was abusing his position of power in relation to the recruits. Julie reported wrongdoing, and Staff Sergeant Hagen should have understood that this was a report of wrongdoing.
- Handling a disclosure in this way may deter other people from raising issues of concern

and prevent the agency from identifying potential wrongdoing.

10.1.2 WO PEDERSEN'S ACTIONS

- Julie has spoken up about possible abuse of power and discrimination that may constitute wrongdoing. This is a serious issue that must be processed in accordance with the rules on whistleblowing. When her immediate superior ignored her concerns, she contacted another leader.
- WO Pedersen must follow up the report of wrongdoing. If he finds it challenging to deal with this on his own, he can consider contacting his immediate superior or the control unit in the armed forces.
- Pedersen must register receipt of the disclosure by creating a disclosure record.
- Pedersen must assess whether immediate measures are required, for example offering support to the whistleblower.
- The person pursuing the report of wrongdoing must assess the case. The aim of this is to ensure that the facts of the case are established within a reasonable amount of time.
- Pedersen must assess when and how Sergeant Johansen is to be informed about the report of wrongdoing that has been submitted, ensuring that this is done before others are questioned.
- Pedersen must evaluate his own impartiality in relation to Julie, Sergeant Johansen and Staff Sergeant Hagen.
- Pedersen must evaluate his own authority to conduct the investigation and obtain suf-

ficient documentation.

- The executive officer can ask the others in the group individually if they would consider participating in a conversation about the group environment in order to identify issues of concern, taking care not to mention the disclosure that has been received.
- The executive officer can investigate whether there is a high rate of sickness absence in the groups for which Sergeant Johansen has had responsibility. A high rate of sickness absence may indicate whether there are underlying issues of concern that need to be examined in greater detail.
- The executive officer must assess whether the complexity and gravity of the case are such that he/she should bring in the control unit or HR.
- After having mapped the case and obtained enough facts to make a responsible decision, WO Pedersen must decide whether Julie has reported wrongdoing.
- On the basis of the findings, WO Pedersen concludes that wrongdoing has been reported. He prepares a final report that he passes up the line for assessment and implementation of follow-up in this case, with the aim of preventing similar cases in the future.

10.2 CASE 2: IMPARTIALITY AND PUBLIC PROCUREMENT

Stian is a middle manager who works in the procurement unit. He receives a phone-call one day from someone who introduces himself as Henrik Hansen. Henrik Hansen says that he is employed in a development company that recently submitted a tender to the Ministry of

Defence in connection with a procurement.

Stian knows which procurement he is referring to and answers that Hilde, his colleague, deals with questions about this. He asks if he should put the caller through to her. Henrik Hansen answers that he is aware that Hilde is the contact person, but there is a reason that he has not contacted her directly.

Henrik Hansen explains to Stian that he has found out that Hilde's husband has ownership interests in one of the companies that has gone on to the next round of the procurement process, and that he understands that it is Hilde who has decided, or at least been involved in deciding which of the bidders should continue to the next round.

Stian is surprised. They have talked several times about the rules on impartiality, and he knows that Hilde is familiar with these. He notes Henrik Hansen's telephone number, thanks him for the information and asks him to keep quiet about this for the time being. Stian tells him that he will deal with the matter and will ensure that steps are taken to rectify the situation.

Henrik Hansen says that he will call Stian if necessary, but that he has no further information other than what he has already given.

10.2.1 STIAN'S ACTIONS

- Stian should regard this as a report of wrongdoing. Reports of wrongdoing can stem from external as well as internal sources, and can take all forms, including telephone communications.
- Hansen implies that wrongdoing may have taken place. If the accusation is correct, a violation of the rules on impartiality in connection with the procurement has occurred.
- Stian should follow up the report immediately. He knows that all disclosures must be taken seriously, regardless of whether they are from an external source.
- Stian should contact his immediate manager to inform him/her about the case.
- Stian can also contact the control unit to ask for advice and guidance.
- Stian must assess his own impartiality, in relation to both Henrik Hansen and Hilde. Since Stian and Hilde are on the same level (both are middle managers), Stian decides to pass on responsibility for dealing with the report to his head of department.
- Stian must provide sufficient documentation of the case.

10.2.2 HEAD OF DEPARTMENT'S ACTIONS

- The head of department to whom Stian passed the case undertakes an assessment of whether he himself is impartial, has sufficient authority and is the right person to process the report or whether it should be passed on to the control unit or some other unit.
- He then assesses whether the gravity of the case indicates that top management should be informed and if it is necessary to take immediate measures.
- The head of department must ensure proper processing of the report and gather as much information as possible.
- The head of department concludes that he

can carry out some investigations without compromising any evidence.

- The head of department must evaluate when and how Hilde should be informed of the report submitted.
- The head of department must carry out an assessment and obtain the facts. The aim of the assessment is to ensure that the facts of the case are sufficiently established within a reasonable amount of time.
- The head of department must ensure that all case processing and decisions are documented and that any paper documents are securely locked away.
- The head of department decides to check the Internet and notes that Hilde's husband is registered as having an ownership interest in the parent company of a firm that has taken part in the procurement process.
- He also checks whether it is correct that the firm has gone on to the next round of bidding and checks the case processing system to see whether Hilde has signed the tender protocol.
- The head of department records what has been done in the case, and attaches the information he has obtained, such as a printout from the Internet and an overview of which bidders have gone on to the next round of the procurement process.
- The head of department asks for a meeting with Hilde at which she is given the opportunity to give her version of the case thus safeguarding her right of contradiction. He also informs her of the right to be accompa-

nied by an counsellor.

- The head of department concludes on the basis of his findings that wrongdoing has been reported. He prepares a final report that is passed further up the line for assessment and implementation of follow-up vis-à-vis the parties in the case. Measures to prevent similar events taking place in the future will also be implemented.

10.3 CASE 3: SEXUAL HARASSMENT

Head of department Tarald is a project manager and has had a meeting with his project team. After the meeting, Katrine, one of the team members, asks if she can have a word with him.

Katrine says that she finds the way Finn, a middle manager in the department, acts towards her and the other women in the department offensive. She explains that he often puts his hand on her shoulder and that he comments on her appearance, body and clothes on a daily basis. This also applies to other women.

Tarald has noticed that Finn pays women a lot of attention, but he has not given more thought to this. He has not viewed this as being offensive to others, and he thinks Katrine may be a bit over-sensitive because she is always bringing things up. Moreover, he does not understand why Katrine is taking this up with him when it is clearly an HR matter.

Tarald becomes aware that to some extent he has adopted a defensive attitude in relation to Finn because he and Finn have become good friends. He was also responsible for appointing Finn as a middle manager, and he is afraid that a complaint about Finn would have a negative impact on how senior management would view his own leadership of the department.

10.3.1 TARALD'S ACTIONS

- Katrine reported wrongdoing to her immediate manager and has reported in accordance with the regulations.
- Since Tarald is a good friend of the subject of the whistleblowing, he should consider whether he is sufficiently objective to deal with the disclosure himself.
- Tarald should follow up the situation. There are several ways of doing this.
- Tarald must evaluate whether he is capable of dealing with the case on his own, or if he should contact the control unit for support.
- Tarald must register receipt of the whistleblowing report and create a disclosure record.
- Tarald decides that he cannot deal with the whistleblowing case on his own and therefore decides to contact Katrine to ask for her permission to transfer the case to the control unit for further processing.
- Tarald must pass on all the documentation he has received or prepared to the control unit, which will pursue the case.

10.4 CASE 4: SUSPECTED CORRUPTION

Gustav, a line manager in an agency, receives an email from Adam Peterson:

'Dear Mr. Gustav,

I am writing to you concerning your sub supplier of Air Force, International Company of Air Force.

I know for a fact that Mr. Arne Andersen, former employee in the Norwegian Ministry of Defence and now CEO in an International Company of Air

Force, has paid an amount of USD 200 000 to a government official in Libya. I am convinced that the transaction involves corruption, and I wanted to inform you of this.

As I am an International Company of Air Force employee, I want to stay anonymous. I am scared that it will lead to retaliation if I try to proceed this internally at International Company of Air Force, and in worst case lose my job.

Adam Peterson'

10.4.1 GUSTAV'S ACTIONS

- Gustav should regard this as a report of wrongdoing. Reports of wrongdoing can come from external as well as internal sources, and in all forms, including by email.
- Whistleblowing procedures state that external persons and others without direct association with the agency have the right to report wrongdoing.
- This must be considered as possible serious wrongdoing (corruption is a criminal offence).
- Gustav must inform his immediate manager. Cases of this type are normally transferred to the control unit.
- When embezzlement, corruption, theft, fraud or misappropriation of funds are reported in the defence sector, point 10.19 of the Personnel Handbook for State Employees applies.
- Gustav and the manager should submit the case to the control unit. When the report concerns a possible criminal offence, it is extremely important that no actions are ta-

ken that can destroy evidence if a criminal case is brought later.

- The control unit must evaluate whether there is an urgent need to introduce measures and inform top management if necessary.
- The control unit registers receipt of the report by creating a disclosure record.
- The whistleblower's identity must not be revealed to more people than absolutely necessary.
- The control unit investigates the matter and prepares a final report.

10.5 CASE 5: HRM CASE VS WHISTLEBLOWING CASE

Lars and Sonja work at the same base and Lars normally functions as Sonja's manager. In addition to their normal work, they have been given key roles in a large project, Sonja as a sub-project leader and Lars as the person responsible for project administration. They have participated in a project status meeting and after the meeting they talk together about the progress of the project.

The conversation turns to one of the team members in Sonja's group, Ari. Sonja says that Ari's work has been far below what could be expected of an employee in such a position and with his background. His work is completely unacceptable, and Sonja is tired of having to work twice as hard to fix what Ari has done.

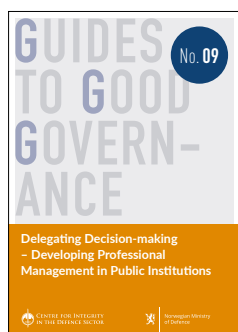
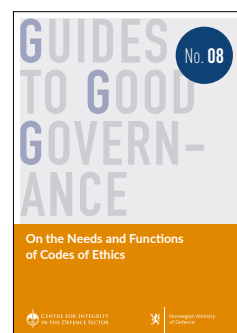
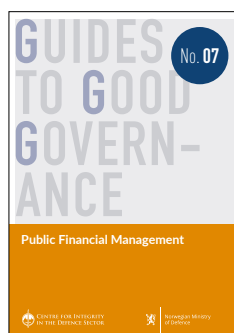
Lars responds that he has never worked directly with Ari but that he too has heard from other project members that Ari's work is not up to the desired standard. When he thinks about it, he has noticed that Ari has had less

to do recently, and wonders if this is perhaps because the project members find it exhausting to work with him because his work is not up to standard.

10.5.1 LARS' ACTIONS

- Sonja has taken up an issue of concern with her immediate line manager, in line with the guidelines on whistleblowing in the defence sector. Reporting wrongdoing in accordance with whistleblowing procedures is always a justifiable action.
- In the conversation, Sonja has mentioned Ari's poor performance in the team while Lars has also heard about the same problem from other project members. The fact that Ari's work is not up to the standard expected must be regarded as an HR matter and not a case of wrongdoing.
- There may be several reasons why Ari's work is not up to the standard expected, and it is important that this is dealt with so that Ari and his colleagues have the opportunity to take the steps necessary. It is possible that Ari will be excluded at the workplace in that he is subject to social exclusion or is not given work tasks.
- Lars invites Ari to take part in a conversation where questions related to his work situation are taken up.
- Lars assesses whether he should deal with the situation. He contacts HR to ask for support. He views this as an HR case and not a report of wrongdoing.
- Lars informs Sonja that the case is being dealt with and makes it clear that she has a duty of confidentiality in this matter.

Guides to Good Governance series



Guides to Good Governance is a series of small booklets each of which discusses a particular topic of importance to good governance in the defence sector. The guides can be read by individuals with an interest in learning more about one or several topics of direct relevance to good governance in the defence sector – or the public sector more generally – and they can be used for educational purposes.

Reproduction in whole or in parts is permitted, provided that full credit is given to the Centre for Integrity in the Defence Sector, Oslo, Norway, and provided that any such reproduction, whether in whole or in parts, is not sold or incorporated in works that are sold.

DSS publikasjonsnummer: S-1032 E

ISBN trykket utgave: 978-82-7924-105-8

ISBN elektronisk utgave: 978-82-7924-107-2

Published by: Centre for Integrity in the Defence Sector

Design: www.melkeveien.no

Print: Norwegian Government Security and Service Organisation

November/2020. Impressions: 100



CENTRE FOR INTEGRITY
IN THE DEFENCE SECTOR

www.cids.no