
Tell us your concern Guideline

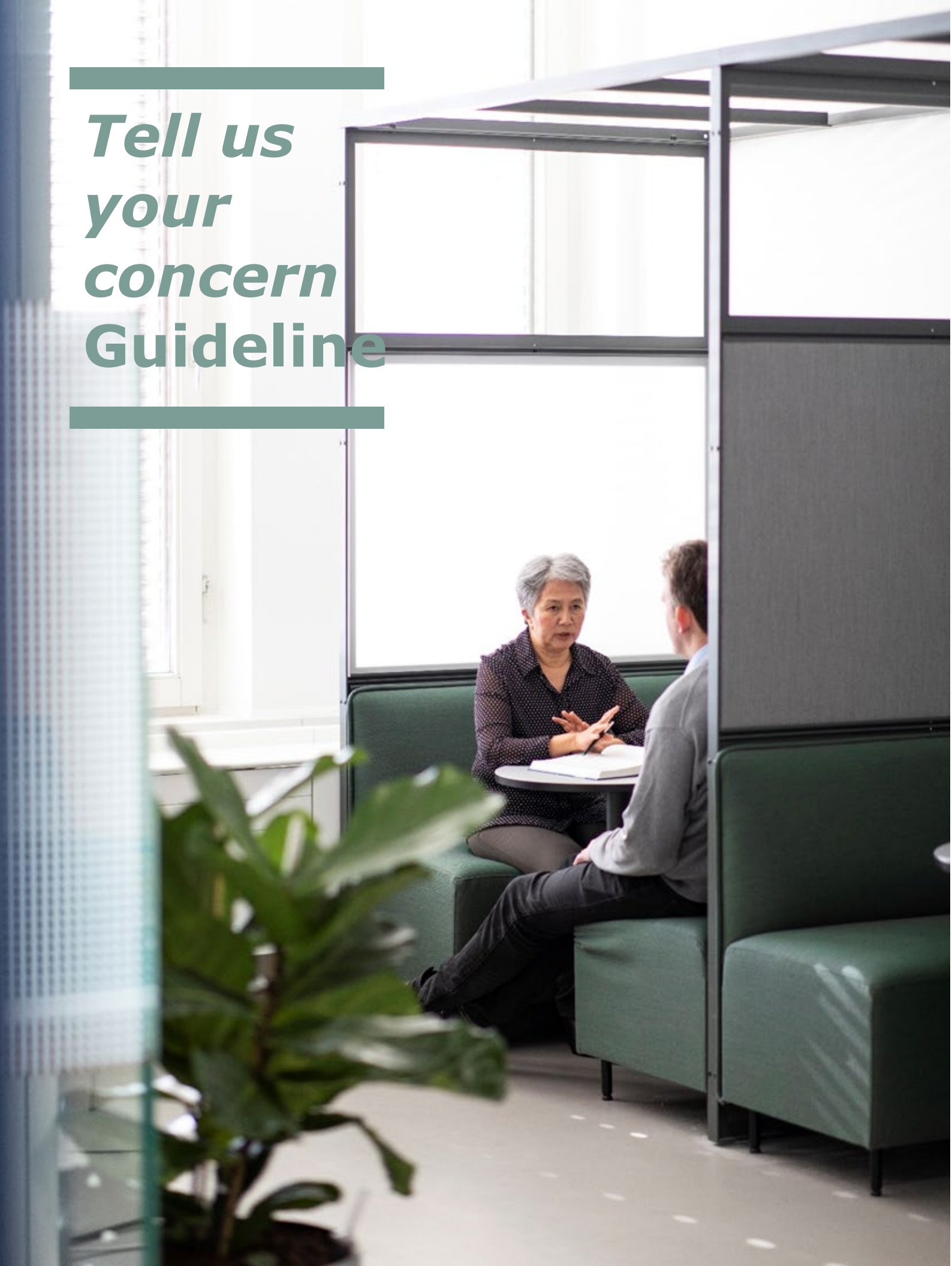


Table of contents

1	Purpose	2
2	What matters can be reported?	3
3	Who can submit a whistleblower report?	4
4	When should you consider making a report?	5
5	How do you make a report?	6
6	What should be included in the report?	7
7	How is my report processed – and by whom?	8
8	What and when can I expect to hear from COWI?	10
9	Is the subject of my report informed of it?	11
10	Personal data	12
11	Who has access to my report and the information/data in the report?	13
12	How am I protected against retaliation?	14

1 Purpose

COWI has established a whistleblower program, the *Tell us your concern* program, covering the COWI Group, in order to enable whistleblowers to report concerns or reasonable suspicions about actual or potential compliance breaches, which occurred or are very likely to occur and about attempts to conceal such breaches.

Whistleblowers are encouraged to report such suspicions and concerns as soon as possible in the knowledge that they are able to do so without fear of reprisals, retaliation, intimidation, harassment, discrimination or adverse employment consequences because of such a report.

The purpose of this guideline is to provide you with the practical details of the use, scope and administration of COWI's *Tell us your concern* program. If you are considering submitting a compliance concern/whistleblower report, it is our hope and aim that this guideline gives you as much information as you may need for these considerations.

The guideline applies to all concerns or reasonable suspicions, whether reported through the *Tell us your concern* hotline or raised internally in COWI through other channels.

2 What matters can be reported?

The *Tell us your concern hotline* policy and *Tell us your concern* program guideline covers reporting of non-compliance with EU law as defined in the Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law and covers reporting of serious breaches of applicable law or regulations or other serious matters including the following:

- Criminal offences, including fraud, embezzlement, misuse of assets, forgery of documents, accounting manipulation, bribery and corruption, theft, money laundering and terrorist financing
- Serious and/or repeated breaches of internal rules, policies and guidelines in COWI
- Discrimination, bullying, harassment, racism, violence, threats and sexual abuse
- Breach of environmental regulations and laws
- Competition law breach and public procurement law breach
- Serious or repeated breach of occupational health and safety legislation
- Conflict of interest
- Breach of professional secrecy
- Breach of protection of privacy and personal data
- Retaliation
- Matters against the public interest

The above are only examples. If you are in doubt as to whether or not the report falls within the scope of this guideline, you are encouraged to use the *Tell us your concern* program. All reports made through the program will be assessed. Reports that fall within the scope of the program will be handled as whistleblower reports.

Less serious matters such as dissatisfaction with terms of employment, office rules, difficulties in cooperation (internal as well as external) and disagreement on professional solutions should not be reported through COWI's *Tell us your concern* hotline but you are encouraged to report these matters to COWI's leaders at an appropriate level.

The subjects of the reportable matters must be either COWI as an institution or individual COWI employees, officers, directors, board members, etc.

3 Who can submit a whistleblower report?

COWI's *Tell us your concern* program is primarily intended for use by COWI Group employees and COWI's partners such as its customers, suppliers, collaborators and sub-consultants.

But, in practice, COWI's *Tell us your concern* hotline is accessible for everyone, even those not included in the list above such as former employees and job applicants.

COWI Group employees

COWI has an open management culture, and as a COWI employee you are encouraged to consult your local P&O Partner or your leaders if you have knowledge of or concerns about misconduct regarding any of the reportable matters listed in this guideline.

However, if you do not believe reporting to P&O or management will work – or feel uncomfortable doing so – you can report your concerns through COWI's *Tell us your concern* hotline.

COWI's business relationships and other stakeholders

If you represent a business relation to COWI or otherwise through a current or previous affiliation with COWI find or suspect a reportable matter, we encourage you to inform us, preferably directly to COWI's management at an appropriate level, or alternatively through COWI's *Tell us your concern* hotline.

4 When should you consider making a report?

Anyone reporting a concern under COWI's *Tell us your concern* program must be acting in good faith and must have reasonable grounds for believing that the information reported is true and accurate.

You are encouraged to make a report if you have knowledge of or reasonable concerns about actual or potential reportable matters which have occurred or are likely to occur.

Your considerations should be based on factual knowledge or objective criteria regarding the reasons for your concern, preferably substantiated by any available relevant documentation. Reports based solely on rumors or completely unsubstantiated allegations or suspicions should be avoided.

However, it is important to emphasize that your report does not need to provide actual proof of your knowledge or concern, and that your report, provided it is submitted in good faith and that you have reasonable grounds for believing that the information reported is true and accurate, still qualifies you for protection even if your allegations turn out to be incorrect.

While you are encouraged to report under COWI's *Tell us your concern* program, you may also decide to use the external whistleblowing reporting schemes set up by the authorities in the EU. A list of country specific reporting channels can be found in the following link:

<https://www.navex.com/en-gb/how-to-file-whistleblower-report-eu/>

5 How do you make a report?

COWI's *Tell us your concern* hotline is easily accessible on www.cowi.com and www.arkitema.com.¹ and ²

For COWI Group employees, links to the *Tell us your concern* hotline are also placed on the front page of the internal COWI portal.

¹ Specifically for reports submitted in Sweden, oral reporting via the whistleblower platform, EthicsPoint, is an option.

² The Danish Data Protection Agency, the Polish Ombudsman and other Polish authorities as well as several Swedish authorities (e.g. Integritetsskyddsmyndigheten, Arbetsmiljöverket, Konkurrensverket and Ekobrottsmyndigheten) have set up external whistleblower reporting lines available for reporting on specific different matters. These external reporting lines have primarily been set up in the interest of whistleblowers wanting to report on matters about companies that do not have a whistleblower scheme of their own.

6 What should be included in the report?

You should provide as much detailed and relevant information as possible for COWI to thoroughly investigate your report.

Examples of useful details:

- Date, time and location of the reported matter
- Name(s) of person(s) involved, roles and, if relevant, the involved project
- Your relationship with the person(s) involved
- The general nature of your concern
- How you became aware of the reported matter
- Possible witnesses
- Other information that might support your concern.

You can choose to be anonymous in your report, but COWI encourages you to provide your name and contact details, as this makes it easier for COWI to address your concern.

7 How is my report processed – and by whom?

Your report submission is received in a specialized whistleblower IT system called EthicsPoint, which is operated by NAVEX, an independent third-party company that hosts COWI's whistleblowing database. NAVEX informs COWI's Business Ethics Manager and General Counsel of the incoming report.

If a report concerns the Business Ethics Manager, its submission will be referred solely to the General Counsel.

If a report concerns the General Counsel, its submission will be referred solely to the CFO.

Upon submission of your report, you are assigned a unique code called a 'report key' and you are asked to create a password to access your report in EthicsPoint. Write down your report key and password and keep them in a safe place.

When you log in to EthicsPoint, you can track your report, receive follow-up information and feedback, provide additional information, etc.

If you choose to be anonymous, it is particularly important that you regularly log in and check your report as this is the only channel available for COWI to provide feedback and ask for additional information.

If the report does not fall within the scope of this guideline, the whistleblower will be notified of this.

If the report falls within the scope of this guideline, the General Counsel will decide if there is a basis for conducting an investigation and determine the appropriate steps to take on the basis of the report. The General Counsel is also authorized to take all other follow-up actions as part of the investigation of a report, including further communication with the whistleblower, requesting additional information and providing feedback to the whistleblower. The General Counsel may involve or delegate all or some of these actions to the Business Ethics Manager.

It may be necessary to involve experts from Group Finance, IT, P&O Business Partners, the Managing Director of the COWI Group company or external investigation experts where the reported circumstances have occurred to ensure that the necessary skills and local expertise are present to conduct an independent, professional and objective investigation.

The investigation is conducted independently, with due diligence and in a confidential manner to the maximum extent, consistent with a thorough and complete investigation.



A summary in the form of a presentation of all reports received is submitted to the CEO, the CFO, the Executive Leadership Team and the Audit Committee as well as the Board of Directors. The General Counsel may involve Head of the Executive Office for reporting purposes.

8 What and when can I expect to hear from COWI?

Once you have submitted a report, you will receive confirmation of its receipt within seven days through the whistleblower system.

Subsequently, COWI will follow up as regularly as the specific report requires, informing you about any action taken by COWI to assess the accuracy of your report and, where relevant, to address the reported matter, including actions such as an internal enquiry or investigation, prosecution, action for recovery of funds or closure of the investigation.

All investigations will be conducted in a timely manner and, to the extent possible, completed within 90 days of receiving your initial report. You will receive thorough feedback on your report once the investigations have been completed. If the investigations cannot be completed within 90 days you will be notified hereof.

9 Is the subject of my report informed of it?

Individuals who are subject to a formal investigation because of your report may be informed once we have received the report and initiate the investigation.

However, such information takes due consideration to the confidential nature of your report and will be done in such a way that the investigation is not compromised.

In case of significant and legitimate interests, including the whistleblower's and the individual's own interests, or if the purpose of the investigation necessitates it, the notice will be postponed or omitted. Further reference is made to COWI's Privacy Notice.

10 Personal data

The legal basis for processing such personal data follows from Regulation (EU) 2016/679 ('**GDPR**'), Article 6 (1) on the processing of personal data, Article 9 (2) on the processing of special categories of personal data, and Article 10 on personal data relating to criminal convictions and offences, if it is necessary to process and handle a whistleblower report.

Furthermore, companies are subject to any local laws relating to personal data protection of the countries in which they operate.

All reports will be stored securely, and the information will be limited to as few people as possible.

Data subjects can forward comments or questions about the processing of personal data to COWI.

Further reference is made to COWI's Privacy Notice for Employees and general Privacy Notice that applies to external parties.

11 Who has access to my report and the information/data in the report?

Access to the data in EthicsPoint is restricted to the following users:

- Group CFO,
- General Counsel,
- Business Ethics Manager,
- Head of the Executive Office (limited case view for reporting purposes only),
- P&O Business Partners (limited access to assigned cases only),
- Group Finance Partners (limited access to assigned cases only)
- COWI's external lawyer (limited access to assigned cases only)
- External forensic experts (limited access to assigned cases only)
- NAVEX, COWI's EthicsPoint system provider, also has access to data in the EthicsPoint system for administrative purposes.

The scope and terms of NAVEX's access and services in general are covered in a separate data processing agreement. NAVEX stores EthicsPoint data and takes all reasonable precautions to protect personal information in its possession from loss, misuse and unauthorized access, disclosure, alteration and destruction.

COWI obtains an independent auditor's report annually ensuring that NAVEX adheres to necessary security measures. COWI will further exercise its audit rights with NAVEX, if deemed appropriate.

Collection and processing of data in the EthicsPoint system and any subsequent investigations follow applicable legislation and principles of proportionality and reasonable measures.

During the investigation of your report, data is only processed by individuals necessary for the successful conclusion of the investigation.

If the case is transferred to the authorities, the information will be kept until the authorities have closed the case.

All external electronic lines of communication as well as all electronic transfers of sensitive data regarding your report are encrypted.

12 How am I protected against retaliation?

COWI will not accept any kind of retaliation or unfair treatment of you because of your report, provided it is submitted in good faith and that you have reasonable grounds for believing that the information reported is true and accurate.

This means that any COWI employee who engages in retaliation such as discharge, demotion, suspension, threats, harassment or any manner of discrimination against you, whether directly or indirectly, or anyone who encourages others to do so, may be subject to disciplinary action, including, if necessary, termination of employment.

If you believe that you have been retaliated against for reporting or participating in an investigation, including threats or attempts of the same, you should immediately report such perceived retaliation to COWI's Business Ethics Manager. All such attempts at retaliation will also be investigated confidentially to the maximum extent possible.

However, protection is not eligible for those utilizing COWI's *Tell us your concern* program to knowingly submit a report containing misleading or false concerns or allegations.