

Speak-Up Policy CM.com N.V.

Purpose

The management board of CM.com N.V. (the "Company") has adopted this Speak-Up Policy. This Speak-Up Policy is intended to encourage everyone within the Company to speak-up about any suspected misconduct, irregularity or incident. This Speak-Up Policy sets out which and how matters should be reported, the procedure that is followed once a report has been made, and how individuals' reporting concerns are protected.

The Company is committed to conducting business in compliance with applicable laws and regulations and the Company's codes and policies. Therefore, it is important that the Company is aware of possible violations. This Speak-Up Policy has been established in accordance with the House for Whistleblowers Act, the degree on Conduct of Business Supervision of Financial Undertakings and the Dutch Corporate Governance Code and was adopted on 21 February 2020 and adjusted on 18 March 2022. This Speak-Up Policy is published on the Company's website.

Who can report?

This Policy applies to individuals who acquired information on breaches or are subject to misconduct in a work and business-related context. It does not matter whether the work-based relationship is yet to begin, is actual or has since ended. This includes but is not limited to workers, self-employed persons, shareholders, volunteers, trainees, (sub)contractors, partners and suppliers.

Which concerns are covered by this reporting policy?

This Policy can be used to report concerns about suspicions of possible misconduct or irregularities within the Company ("Misconduct"). These concerns may relate to the following matters:

- Criminal offence or violation of the law;
- Violation of the Company's internal policies and/or procedures;
- Human Rights violations;
- Dishonesty or unethical behavior;
- Discrimination and harassment;
- Irregularities regarding accounting, internal accounting controls or auditing matters;
- Bribery and corruption;
- Threats to the environment;
- Disclosure of confidential information;
- Retaliation against any person for speaking up or becoming otherwise involved under this policy;
- Any other any other concerns if it feels appropriate.

An Individual's report of suspicions of possible Misconduct should be supported by relevant information and submitted in good faith. An individual does not need to be certain that Misconduct has taken place to speak up.

Who can I report to and how?

Individuals can choose to report matters in writing, orally by phone or in person. Individuals are encouraged to first address and discuss the matter with the individual(s) concerned. If for any reason, the Individual does not feel comfortable in doing so, the matter can be reported to their (direct) Lead, HR Business partner or Risk & Compliance managers.

Individual concerned

(direct) lead,
HR business partner
or Risk & Compliance
managers

Confidential advisor

External Speak-Up
application

However, if for any reason this is not appropriate, the Individual can raise his or her concern to an external confidants (part of the HQ care-team) (the "Confidential Advisor"), or via the external Speak-Up application.

For employees, more details of the Care team and the external Confidential Advisors can be found on [Business Support](#). If requested by the individual, the Confidential Advisor may inform the HR Business partner or Reporting Officer to take the matter further, but only in consultation with the reporter. In that case, a report will be submitted. The Reporting Officer is the head of Risk & Compliance.

Via the Speak-Up application it is possible to report any suspicions by text or voice message in any language which will be automatically translated to the language of the Reporting Officer. Reports made via the Speak-Up application are accessible to and will initially be followed up a limited number of people from the Risk & Compliance team.



This tool is accessible via three ways:

1. Download the application "SpeakUp by People InTouch" in the App Store or Google Play and scan the QR-code;
2. Scan the QR-code with your camera and report via your web browser.
3. Go to <https://cmcom.speakup.report/speakupline>

If the Reporting Officer is involved in the suspected Misconduct, one of the other reporting lines may be used. When the suspicion relates to management of the Company the Reporting Officer will involve the Supervisory Board. The Reporting Officer is responsible for the follow up on any reports and for the Speak-Up Register.

Can I ask someone for advice?

When an individual is not certain that Misconduct has taken place to speak up, has any questions or is looking for advice, all above persons and tools can be used.

Can I remain anonymous?

The Company encourages an open culture and emphasizes the importance of Individual raising any concerns openly to assess, investigate and gather additional information, if required. However, if an Individual has serious objections to openly raise concerns and wishes to remain anonymous, the Company will use all reasonable efforts to ensure an Individual's anonymity (unless the Company is required to comply with a competing legal or regulatory obligation).

What happens after I report a concern?

The Company takes every report of suspicions of possible Misconduct seriously. After submitting a report, the Individual receives a confirmation of receipt of the report within 48 hours.

Depending on the report, the Reporting Officer or a by the Reporting Officer designated person will carry out an initial assessment to determine how the report should be followed up, and investigated where appropriate. Depending on the type of report this could be for example someone of the Risk & Compliance department, the Legal department or HR department. Where possible, the reporting officer will inform the Individual of the outcome of this assessment. The reporting officer may request additional information from the Individual at this time.

The Company intends to give the Individual an indication of how the Company will deal with the report, the expected timeframe, the results of the investigation and any actions taken in response. As soon as possible, but at least within three month after the reporting, the Individual receives information about the assessment of the report and where applicable the follow-up of the report. However, the need for confidentiality and privacy and other considerations may prevent the Company from being able to give the Individual (specific) details regarding the investigation or any remedial and disciplinary action taken as a result. Any information shared with the Individual about the investigation and action taken must be treated as confidential.

The Company cannot guarantee the outcome expected or desired by the Individual. However, the Company is committed to dealing with the Individual's genuine concerns fairly and appropriately.

Will my report be treated confidentially?

The Company will treat any report confidentially in order to allow for an adequate investigation of the report and to comply with applicable privacy laws.

An Individual may indicate that his or her report should be treated anonymously. The name of the Individual who submitted a report in good faith will not be disclosed to others within or outside the Company unless the Individual gives his or her prior written consent or the Company is required to comply with a legal or regulatory obligation. The Individual is entitled to deny or withdraw his or her consent at any time and must be informed of this right prior to giving consent.

The information received will only be shared with others within or outside the Company if and to the extent this is required to appropriately deal with the report and the issues raised in it. Again, the name of the Individual will not be disclosed unless the Individual has given his or her consent or there is a legal or regulatory obligation to do so.

The Company will generally notify the person implicated in a report that concerns have been raised in relation to him or her. The Company will make this notification within a reasonable time and take into consideration the interests of the investigation. The Company will take all reasonable measures to prevent that the person implicated in a report from learning the identity of the Individual who submitted the report.

If it turns out the report was not made in good faith, the Company is not bound by these confidentiality undertakings, without prejudice to applicable privacy laws.

How will I be protected if I report a concern?

No Individual who in good faith raises a concern involving matters covered by this Speak-Up Policy will suffer harassment, retaliation or any other adverse (employment) consequences as a result of raising a concern. The Company will not tolerate any form of threat or retaliation, and will take (disciplinary) action against relevant co-workers or managers where appropriate.

An Individual who believes he or she has been penalized because of the Individual's status as a reporter of suspected Misconduct or due to participation in the investigation of a report is encouraged to immediately report such conduct to allow the Company to take appropriate remedial measures. The above mentioned channels may be used, for which the reporter may consider to use another channel than initially used.

The Company may only take disciplinary actions if the Company concludes that a report has not been made in good faith, e.g. because false allegations have been made knowingly, improperly, maliciously, or for personal financial gain.

If it turns out that the Individual has been personally involved in suspected Misconduct, reporting such Misconduct does not exempt the Individual from possible (disciplinary) actions by the Company or civil, criminal or regulatory liability. In its actions, the Company will, however, at all times take into consideration that an Individual has voluntarily and in good faith reported the suspicions of Misconduct through this Speak-Up Policy.

Can I report concerns outside the company?

Individuals are encouraged to report their concerns internally. In exceptional circumstances special rules apply where suspicions of misconduct can be reported outside the Company. As these institutions differ per country, more guidance is included in Appendix A.

Administration

The Owner of this Policy is responsible for the administration, revision, interpretation, and application of this policy. The Policy will be reviewed annually and revised as needed.

Privacy

If an Individual submits a report under this Policy, and via the speak-up application, personal data will be processed by the Company. The personal data processed following this Speak-Up Policy will be limited to personal data which are strictly and objectively necessary to verify the legitimacy of the report and the allegations made. The following personal data will be processed. If provided by the Individual, their name, surname, mailing address, telephone or mobile number and/or email address. The report submitted may also include personal data such as information on the reported person and other third parties involved. This data will be included in the mandatory reports register of the Company.

The personal data will be processed for the period of time strictly and objectively necessary. For the personal data of the reporter, this is usually within 28 days of completion of the investigation of the facts alleged in the report. Such periods would be different when legal proceedings or disciplinary measures are initiated against the reported person or the reporter in cases of false or slanderous declaration. In such cases, personal data should be kept until the conclusion of these proceedings and the period allowed for any appeal.

For the personal data of the reported person, this is usually five (5) years in those cases where the contractual relationship with the Company (if applicable) terminates.

In this case, the Company will keep any relevant personal data that the Company may need to defend itself against any claim(s), challenge(s) or other such action(s) for such time as is necessary.

Where personal data is no longer required by the Company, the Company will either securely delete or anonymize the personal data in question.

By accessing and using the Speak-Up application in an identified manner, the reporter agrees to the processing of their personal data. If the reporter wants to exercise his or hers personal data rights, he or she should not hesitate to contact the Reporting Officer. The Company will verify whether it is possible to accommodate the request and respond as soon as possible and no later than one month after the Company has received the request.

Document Control

Owner	Jorg Voeten, Head of Risk & Compliance
Classification	Public
Approval date	18 March 2022
Approved by	Jörg de Graaf
Company scope	CM.com N.V.
Document reference	

Version control

Revision	Change details	Release date	Author
1.0	First version of Whistleblower policy.	21-2-2021	Head of Legal
2.0	Renamed Whistleblower policy to Speak-Up Policy, implemented changes following of the new directive and included a Speak-Up application as new reporting line.	18-3-2022	Fraud Manager, Head of Legal, Head of Risk & Compliance

Appendix A – Reporting outside the company

The Netherlands

Individuals are encouraged to report their concerns internally. In exceptional circumstances Special Dutch rules apply where Suspicions of misconduct involving the Public Interest or breaches of the Union act (as defined below) can be reported outside the Company to the Institute for Whistleblowers (Huis voor Klokkenluiders) or to an designated authority.

“Suspicions of misconduct involving the Public Interest” should meet the following criteria:

- a) suspicions that are based on reasonable grounds, arising from knowledge acquired by the Individual in working for the Company or arising from knowledge acquired by the Individual through work activities within another company or organization; and
- b) suspicions that involve the public interest because of the violation of laws and regulations, or threats to public health, the safety of individuals, the environment, or the proper functioning of a public service or a company as a result of improper actions.

“Breaches of the Union acts” should meet at least one of the following criteria:

1. breaches falling within the scope of the Union act concerning the following areas:
 - public procurement;
 - financial services, products and markets, and prevention of money laundering and terrorist financing;
 - product safety and compliance;
 - transport safety;
 - protection of the environment;
 - radiation protection and nuclear safety;
 - food and feed safety, animal health and welfare;
 - public health;
 - consumer protection;
 - protection of privacy and personal data, and security of network and information systems;
2. breaches affecting the financial interests of the Union;
3. breaches relating to the internal market, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

If an external report is to be made, it should be made to a competent regulator and in an appropriate manner taking into consideration the legitimate interests of all involved. Except in rare circumstances, reporting matters to the press or on social media will not be appropriate or permissible.

Given the possible severe consequences of external reporting, Individuals are encouraged to seek advice before reporting any concern outside the Company. They can do so with the Confidential Advisor. In the Netherlands, Employees can also consult the advisory department (afdeling advies) of the Institute for Whistleblowers (Huis voor Klokkenluiders).

In addition, in the cases where an external report could be made under this article, an Individual can report a Suspicion involving the Public Interest to the investigation

department (afdeling onderzoek) of the Institute for Whistleblowers. For more information regarding the Institute for Whistleblowers and its procedures, please consult the website <https://www.huisvoorklokkenuiders.nl>. Breaches of the Union Act can be reported to the following authorities, depending on the nature of the breach:

- Authority for Consumers and Markets (de Autoriteit Consument en Markt);
- Authority for the Financial Markets (de Autoriteit Financiële Markten);
- Data Protection Authority (de Autoriteit persoonsgegevens);
- De Nederlandsche Bank N.V.;
- Health and Yought Care Inspectorate (de Inspectie gezondheidszorg en jeugd);
- The Dutch Healthcare Authority (de Nederlandse Zorgautoriteit);
- Authority for Nuclear Safety and Radiation Protection (de Autoriteit Nucleaire Veiligheid en Stralingsbescherming).
- Institute for Whistleblowers;