SPEAK UP POLICY GUIDANCE

Coca-Cola Europacific Partners

POLICY INDEX

Contents

1. Practical Guidance

This Policy Guidance shall apply in all countries (with the exception of Australia) in which CCEP operates as a company-wide Policy.

The purpose of the Policy is to make reporting and the following procedures as easy, understandable and accessible as possible.

SPEAK UP

We encourage reports on any suspected, actual or potential violations of the law, our Code of Conduct, CCEP Policies and other unacceptable conduct (to be referred to as "**potential violations**"), which may be related to CCEP, whether involving our people or third parties working for us or on our behalf.

WHISTLEBLOWING

When you want to report a protected matter under your local whistleblower protection laws or regulations, make sure to familiarise yourself with the applicable reporting ways and which matters fall under this protection. You can find more specific information for your country in the respective country specification annexed to this Policy Guidance.

Who can make a report?

Our internal Speak Up Resources and external Speak Up Channels are open for any person (CCEP-workers and to everyone else connected to CCEP through a current or former work-related context) who seeks to report a potential violation.

What can be reported?

We encourage reports on any potential violations, which may be related to CCEP, whether involving our people or third parties working for us or on our behalf.

When to report ?

We expect that you report as soon as possible after you became aware of the potential violation.

How to report?

You may seek advice from your line manager about potential violations at CCEP and/or raise a report through our internal Speak Resources and/or external Speak Up Channels. We encourage you to reach out to our Speak Up Resources and/or Speak Up Channels first before using other ways of reporting (such as public authorities or press).

Data protection

CCEP is committed to complying with applicable data protection and privacy legislation, as detailed in our privacy and data retention policies.

No retaliation and confidentiality

We **DO NOT** tolerate any form of retaliation, including the threat or attempt of retaliation, against any reporting person or other connected persons for making a report in accordance to this Policy Guidance or for cooperating in an investigation.

Your identity and other non-public information you share in relation to the report will be treated confidentially to the extent possible.

1.1. Introduction

We strongly encourage you to read this Policy Guidance carefully and raise your concerns accordingly. Operating in accordance with our Speak Up Policy and Policy Guidance helps maintain the reputation of CCEP and the continued success of our business.

1.2. Who can make a report?

Our internal Speak Up Resources and external Speak Up Channels are open for any person (CCEP-workers and to everyone else connected to CCEP through a work-related context) who seeks to report a potential violation.
This includes:

- ✓ Workers, whether employed directly by CCEP, engaged through a staffing agency, or are self-employed,
- ✓ Shareholders and persons belonging to our administrative, management or supervisory bodies, including non-executive members, as well as volunteers and paid or unpaid trainees,
- ✓ Any person who acquired information on suspected misconduct in a work-based relationship which has since ended, or who acquired the information during the recruitment process or other pre-contractual negotiations,
- ✓ Any person working under the supervision and direction of our contractors, subcontractors and suppliers,
- ✓ Facilitators, relatives and related entities.

1.3. What to report?

We encourage reports on any potential violations, which may be related to CCEP, whether involving our people or third parties working for us or on our behalf.
Examples of types of potential violations to be reported using this policy:

- ✓ Violation of CCEP's Code of Conduct, or other policies,
- ✓ Fraud, bribery or corruption,
- ✓ Discrimination, racism, harassment, modern slavery,
- ✓ Violation of health and safety procedures,
- ✓ Tax evasion,
- ✓ Conflicts of interest,
- ✓ Human Rights violations,
- ✓ Any act which may harm CCEP's vital interest or reputation.
- ✓ Any impropriety under any local legislation.

Note.
If the matter relates to a workplace dispute or grievance, then you should raise it with your line manager and/or a member of People & Culture.

1.4. When to report?

When reporting urgent ¨potential violations", which pose an immediate danger to our business, employees, consumers or other persons, such as in the case of health and safety hazards, please follow the guidance of the CCEP Incident Management and Crisis Resolution procedure and ensure to inform your line manager and your BU/Regional Legal VP/country lead as soon as practicably possible.

We expect that you report as soon as possible after you became aware of the potential violation. This allows our company to deal with the issue in an early stage and minimise the adverse consequences that may otherwise occur.

Reports should always be made in good faith. This means that at the time of reporting, you have reasonable grounds to believe or suspect that the information indicating the potential violation is true.

1.5. How to report?

Speak Up Channels can be accessed here: https://view.pagetiger.com/speak-up-resources-and-channels

A report may be made through one of our internal Speak Up Resources or our external Speak Up Channels:

- ✓ A Member of your senior local company management,
- ✓ Your local People & Culture Representative or the People Services Team,
- ✓ A member of your local Code of Conduct Committee,
- ✓ A member of the Legal or Ethics and Compliance Team,
- ✓ The Chief Compliance Officer,
- ✓ The General Counsel,
- ✓ Our **external Speak Up Channels.**

We strongly encourage all of our people to share any doubts and concerns relating to potential violations internally within our organisation. However, if sharing doubts or concerns in this way is not practicable or desirable, we encourage reporting through our external Speak Up Channels or relevant local authorities.

Our external Speak Up Channels.

In all our countries we have set up our external Speak Up Channels. They are hosted externally by a third party and provide an additional resource where CCEP employees and everyone else connected to CCEP through a work-related context can ask questions and voice concerns confidentially and anonymously, where allowed by local law. The external Speak Up Channels are available 24 hours a day, 7 days a week and in multiple languages.

The use of CCEP's external Speak Up Channels is not mandatory. Alternative ways exist for asking questions or raising concerns – our internal Speak Up Resources. Work-related grievances can be raised with your line manager and/or a member of People & Culture.

To make an eligible disclosure and be protected by Whistleblower laws, regulations or policy applicable for your territory, please make sure to carefully read the sections applicable for your territory.

1.6. Information to provide

When reporting potential violations, we encourage you to share all information known to you in relation to the potential violation in a detailed manner, and to provide (or refer to) any evidence or supporting documents. This would allow us to handle your report as quickly and effectively as possible.

Please be as detailed and precise as possible. If the report is made orally, you shall have the right to check and rectify the contents of the notes.
When describing the issue, please think about the following questions:

- ✓ What happened or is about to happen?
- ✓ Who is involved?
- ✓ When did or will it happen?
- ✓ Where?
- ✓ What evidence exists to support it?
- ✓ Where can it be found?
- ✓ Who may be able to share relevant information on it?
- ✓ Would you agree that we contact you discreetly to discuss?
- ✓ How can we contact you?

1.7. Anonymous reporting

We believe in honest and open communications. Therefore, when making a report, we encourage you to identify yourself by providing your name, function, and contact details.
This will allow the CCEP staff handling the report to contact you for a follow-up if necessary:

- ✓ Knowing your identity enables us to handle the report more effectively

- ✓ Please note that all our reports are handled in a safe and confidential manner as far as reasonably practicable unless this is not allowed or required by law and/ or risks the investigation by national authorities or judicial proceedings.

- ✓ That said, if you prefer to report anonymously (where allowed by local law), that is not a problem. We are there to handle your concern and will do our best to manage it efficiently, with secrecy, sensitivity and care.

1.8. How do we handle your report?

Once a report is made through our external Speak Up Channels, the following steps will be taken:

1. Reports through CCEP external Speak Up Channels are saved directly on the EthicsPoint server (EU Business Units) and KPMG FairCall (API Business Units), which is highly secure.
2. For EU Business Units, when making a report through our external Speak Up Channels, you will be provided with a case number and asked to create a password. This must be used for further communication – so please make sure to note the information in a secret place. With this case number and password, you will be able to log into the reporting website to obtain feedback and / or updates on your report. The system will enable you to provide additional information to change or supplement your report. In addition if you identified yourself when making the report, we may contact you directly to provide feedback and updates.
3. For API Business Units, when making a report through our external Speak Up Channels, via our webform you will be provided with a case number and asked to create a password. This must be used for further communication – so please make sure to note the information in a secret place. With this case number and password, you will be able to log into the reporting website to obtain feedback and / or updates on your report. The system will enable you to provide additional information to change or supplement your report. In addition if you identified yourself when making the report, we may contact you directly to provide feedback and updates.
4. Within 24 hours, if possible, your report will be shared with our internal team authorised for handling reports.
5. Once we received your report, we strive to acknowledge this receipt within 7 days.
6. Our internal team will conduct an initial assessment and decide upon next steps. When needed, an investigating team will be assigned to review the matter further.
7. When needed, our internal team may ask additional questions or share feedback with you.
8. Our internal team will monitor the handling of the report by the investigation team assigned to act on it.
9. We expect that within three months from the acknowledgement of receipt, we will be providing you with feedback in relation to your report where this is reasonably practicable.
10. When justified, we will take appropriate corrective actions.
11. In certain limited circumstances, CCEP may need to disclose your identity. This may happen when certain obligations are imposed by law. In such cases, we will make sure to apply appropriate safeguards, and to share the disclosure with you in advance, explaining the reasons that justify it, unless this is not allowed or required by law and/ or risks the investigation by national authorities or judicial proceedings.
12. Personal data will be kept as long as necessary to process and investigate the report, or, if applicable, as long as necessary to initiate sanctions or to meet any legal or financial requirement. In any case, if judicial or disciplinary proceedings are initiated, including the necessary time for those proceedings and appeal, the personal data provided will be kept until those proceedings are definitively closed; if not, they will be kept no longer than necessary in line with privacy legislation, in

Europe that is no longer than 2 months after the end date of the investigation and in API Business Units (TBC).

1.9. No retaliation

At CCEP we DO NOT tolerate any form of retaliation, including the threat or attempt of retaliation, against any reporting person or other connected persons for making a report in accordance with our Speak Up Policy Guidance or for cooperating in an investigation.

What is Retaliation? Retaliation covers any direct or indirect act or omission, which may harm a reporting person due to their reporting of potential violations as a result of a genuine concern. Retaliation includes for instance suspension, dismissal, demotion, transfer of duties, reduction in wage, coercion, unfair treatment, etc.

Who is protected? The protection applies to the reporting person, as well as to third persons connected with the reporting person (such as colleagues and relatives), anyone who assisted a reporting person in the reporting process, and any legal entity that the reporting person owns, works for or is otherwise connected with in a work-related context.

The protection also applies when the report was made externally to competent authorities and under certain circumstances also when the concern was publicly disclosed.

Should any person at CCEP, contrary to this Policy and Policy Guidance, directly or indirectly engage in retaliation, CCEP will take the necessary measures to stop the retaliation as soon as possible and will, when appropriate, take disciplinary action against those responsible for the retaliation.

1.10. Data protection

Data privacy. At CCEP we are committed to maintaining stringent privacy, data security and retention controls as detailed in our privacy, security and data retention policies. These standards will also apply with respect to all records relating to the reports made in accordance with this Policy and Policy Guidance.

Confidentiality. Your identity and other non-public information you shared in relation to the report will be treated confidentially so far reasonably practicable. Information in relation to your report will only be shared with persons authorised to handle the report subject to applicable legal requirements on a need-to-know basis. Non-authorised staff members will not have access to this information unless necessary.

In some cases, we may need to share the information relating to the report with competent authorities or as part of an internal, regulatory or legal process. When appropriate, we will inform you about that in advance.

You can find more information on how CCEP may process your personal data in CCEP Employee Privacy Notice available on Genie (for CCEP employees and other staff members) and in the Privacy Notice available here and in the Privacy Notice available here (Ethics Point) and here (Kpmg FairCall) (for other stakeholders).

1.11. Concerns on reporting?

When you have any concerns in relation to the application of this Policy and Policy Guidance or to the handling of your report, we encourage you to contact your line manager or one of the Speak Up Resources before considering reporting externally to competent authorities.

Please be aware that local legislation may vary from country to country. Our local Policy Guidance may give more detail about alternative external bodies to whom reports of potential violations may be made in line with local legislation.

2. Processes, roles, responsibilities, details and further guidance

The purpose of this Policy Guidance is to describe the standards, criteria and responsibilities relating to reports on potential violations which may be related to CCEP, whether involving our people or third parties working for us or on our behalf.

3. Policy compliance

As our policies and policy guidance are based on applicable legislation, please note that breach of or non-compliance with this Policy and the related Guidance could lead to disciplinary action being taken – up to and including summary dismissal in accordance with applicable laws and/or internal policies.

Company policies are subject to change and may vary depending on location. If you are ever uncertain which rule or policy you should follow, or if you are concerned that there might be a conflict between applicable law and the guidance within our policy, please consult Employment Practices (P&C) employment.practices@ccep.com. Unless otherwise stated all policies are discretionary and do not confer any country entitlement.

4. Policy Overview

Risk	Risks relating to Whistleblowing
Title of the Policy	Speak Up Policy and Speak Up Policy Guidance
Scope	Company-wide
Policy Owner	Chief Compliance Officer
Initial date of approval	28/05/2019

Revision Date	09/2024
Version	3.0

4.1 Approval of the Policy

The Policy Owner has obtained the required approval of the contents of this policy as set out below.

Department	Name, Function	Date
CCEP's Compliance and Risk Committee	Related to company-wide or functional risk	06/2022

4.2. Effective date and validity

This Policy and Policy Guidance shall apply with immediate effect once it has been approved by the appropriate responsible person within CCEP on the date indicated at the beginning. The date of revision, from which this Policy is effective, is set out in the policy outline section above.

Should some regulations of this Policy become ineffectual because of changing laws in one Country or Business Unit, the remaining will stay effectual.

4.3. Change control

The Policy and the Policy guidance will be revised when appropriate as circumstances change. At minimum this Policy and Policy Guidance should be reviewed on an annual basis.

CCEP intends to notify employees of changes to its policies where possible. However, CCEP reserves the right to change, revise, withdraw or add to its policies, processes, procedures or guidance at any time, without notice if necessary.

Employment Practices keeps a record of all changes to the Policy and Policy Guidance. If you have questions, please reach out to employment.practices@ccep.com.

ANNEX ONE: SPEAK UP POLICY GUIDANCE

Coca-Cola Europacific Partners

Our Speak Up Policy Guidance applies globally. However, for the countries in this annex, additional instructions apply which are detailed below.

A. Papua New Guinea

In section 1.3 (What to report?) the following is added:

The following conduct is considered a violation under Papua New Guinean law:

- ✓ Any criminal offence,
- ✓ Failure to comply with a legal obligation,
- ✓ Miscarriage of justice,
- ✓ Environmental damage,
- ✓ Deliberately concealing any conduct of impropriety.

In section 1.4 (When to report?) the following is added:

Please note that a person who intentionally makes a false or misleading report commits an offence in Papua New Guinea.

In section 1.5 (How to report?) the following is added:

In Papua New Guinea, employees may also report to:

- ✓ A legal practitioner,
- ✓ The Minister responsible for the Whistleblowing Act, or
- ✓ An approved authority within the meaning of the Whistleblowing act.

Please note that in Papua New Guinea, a report is not protected under the Papua New Guinea Whistleblowing Act when the filing of the report itself constitutes committing an offence.

In section 1.9 (No retaliation) the following is added:

Retaliation also includes:

- ✓ Refusing a transfer, and
- ✓ Refusing a reference or being provided with an adverse reference.

No retaliation rights of an employee include:

- ✓ The protection from occupational detriment,
- ✓ Requesting a transfer to another position with the employer in which the employee will not be subject to occupational detriment,
- ✓ Application to a court in a competent jurisdiction for appropriate relief, and
- ✓ Pursuing any other available process for seeking a remedy.

In section 3 (Policy compliance) the last sentence is amended to:

Unless otherwise stated, to the extent provided by law, all policies are discretionary and do not confer any contra entitlement.

B. Portugal

Practical Guidance – Whistleblowing Protections

To benefit from the whistleblower protection under local law, a reporter must make a report regarding a mandatory topic. Please see these topics below:

i. public procurement;
ii. financial services, products and markets, and the prevention of money laundering and terrorist financing
iii. product safety and conformity
iv. transport safety
v. environmental protection
vi. Radiation protection and nuclear safety;
vii. Food safety and security
viii. Food and feed safety, animal health and animal welfare
ix. Public health
x. Consumer protection
xi. Protection of privacy and personal data and security of network and information systems;
xii. An act or omission contrary and detrimental to the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU), as specified in the applicable Union measures;
xiii. Act or omission contrary to the internal market rules referred to in Article 26(2) TFEU, including competition and State aid rules, as well as corporate tax rules

In section 1 (No retaliation and confidentiality) the following is changed:

Your identity and any other non-public information you share in relation to the report will be treated confidentially to the extent possible is changed to: Your identity and the identity of any third parties mentioned in the report will be treated confidentially.

In section 1.5 (How to report?) the following is added:

Please note that you must report to our internal Speak Up Resources or to our external Speak Up Channels before reporting to any external resource, such as an authority.

A reporter is only allowed under Portuguese law to directly report externally (such as to authorities) if:

- There is no internal Speak Up Resource available,
- The internal Speak Up Resource only allows for reports by employees and the reporter is not an employee,
- The reporter has reasonable ground to believe that the breach cannot be effectively known or resolved internally,

- The reporter has initially lodged an internal report without having been informed of the measures envisaged or taken following the report within the time limit of 3 months set out in the Portuguese Law, or
- The breach is a criminal offence or an administrative offence punishable by a fine of more than € 50 000.

In section 1.8 (How do we handle your report?) the following is changed:

Once we received your report, we strive to acknowledge this receipt within 7 days is changed to: The acknowledgement of the receipt of your report is made within 7 days.

We expect that within three months from the acknowledgement of receipt, we will be providing you with feedback in relation to your report where this is reasonably practicable is changed to: Within three months from the acknowledgement of the receipt, we will be providing you with feedback in relation your report.

If not, they will be kept no longer than necessary in line with privacy legislation, in Europe that is no longer than 2 months after the end date of the investigation and in API Business Units (TBC) is changed to: In Portugal, reports are kept for a minimum of 5 years.

To add in section 1.8 the following paragraph:

The reporter may request, at any time, that the obliged entities communicate the result of the analysis carried out on the reported infringement within 15 days after its conclusion.

C. Spain

Practical Guidance – Whistleblowing Protections

The Spanish Whistleblowing Act only protect those who report a violation of European Union Law within the framework set out by Article 2.1 of Directive (EU) 2019/1937 and also actions or omissions that may constitute a serious or very serious criminal or administrative offense. In any case, all those serious or very serious criminal or administrative offenses that imply economic loss for the Public Treasury and for Social Security will be understood as covered by this protection.

In section 1 (No retaliation and confidentiality) the following is changed:
Your identity and other non-public information you share in relation to the report will be treated confidentially to the extent possible is changed to: Your identity and other non-public information you share in relation to the report will be treated confidentially, unless otherwise required by the applicable law.

In section 1.5 (How to report?) the following is added:

You can make your report either orally or in writing. Verbal reports may be made by telephone or through a voice recording system. A face-to-face meeting can also be scheduled within a

term of 7 days at your request. Verbal reports will be documented by means of a recording or transcript subject to your consent. In case a transcript is made, you will have the opportunity to check, rectify and sign it.

In section 1.7 (Anonymous reporting) the following is changed:
Please note that all our reports are handled in a safe and confidential manner as far as reasonably practicable unless this is not allowed or required by law and/or risks the investigation by national authorities or judicial proceedings is changed to: Please note that all our reports are handled in a safe and confidential manner to the extent allowed by applicable law.

In section 1.8 (How do we handle your report?) the following paragraphs are changed:
Once we received your report, we strive to acknowledge this receipt within 7 days is changed to: we will acknowledge its receipt within 7 days unless this may risk the confidentiality of your communication.

We expect that within three months from the acknowledgment of receipt, we will be providing you with feedback in relation to your report where this is reasonably practicable is changed to: We expect that within three months from the acknowledgment of receipt, we will be providing you with feedback in relation to your report, unless applicable legislation requires a different time period, except in cases of special complexity, in which the term may be extended up to a maximum of three additional months.

Personal data will be kept as long as necessary to process and investigate the report, or, if applicable, as long as necessary to initiate sanctions or to meet any legal or financial requirement. In any case, if judicial or disciplinary proceedings are initiated, including the necessary time for those proceedings and appeal, the personal data provided will be kept until those proceedings are definitively closed; if not, they will be kept no longer than necessary in line with privacy legislation, in Europe that is no longer than 2 months after the end date of the investigation and in API Business Units (TBC) is changed to: Personal data will be kept as long as necessary to process and investigate the report or, if applicable, as long as necessary to initiate sanctions or to meet any legal requirement. In any case, data retention periods have been adapted to comply with the applicable Spanish legislation.

To add in section 1.8 the following paragraphs:

If you receive a communication without being in charge of its management, you must guarantee confidentiality and immediately submit it to the System Manager (Ethics Committee).

To add the reference to "Respect for the right to honour of the persons concerned".

In Spain all reports will be handled according to the Whistleblowing Investigation Procedure.

In section 1.10 (Data protection) the following is changed:

Your identity and other non-public information you shared in relation to the report will be treated confidentially so far reasonably practicable is changed to: Your identity and other non-public information you shared in relation to the report will be treated confidentially to the extent allowed by applicable law.

D. Sweden

Section 1 (Speak Up) is replaced by:

We encourage reports on any suspected, actual or potential violations relating to any of the issues for which reporting in Sweden is possible (to be referred to as "potential violations"), which may be related to CCEP, whether involving our people or third parties working for us or on our behalf.

Section 1.3 (What to report?) is replaced by:

In Sweden, our internal Speak Up Resources and external Speak Up Channels can be used to report issues relating to:

- ✓ 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,
- ✓ Financial interests of the European Union or relating to the European Union' s internal market,
- ✓ Misconduct that would be of public interests of being disclosed.

In section 1.5 (How to report?) the following is added:

You are entitled to submit a report externally to the designated national authorities competent to receive and follow-up on reports, through their established reporting channels, for matters falling within the respective authority's scope of responsibility.

All potential violations, except misconduct to be disclosed for the public interest, can be reported to the relevant institutions, bodies, offices or agencies of the European Union in accordance with the terms provided for such channels in the regulations of the European Union.

In Section 1.12 (Constitutional rights) is added:

Please note that the content of this Speak Up Policy Guidance does not have any impact on your constitutional rights under the *Swedish Freedom of the Press Act* and the *Fundamental Law on Freedom of Expression*, involving, for example, a right to freely disclose information to the media and collect information for this purpose. However, please note that the protection from investigations and reprisals following such disclosure, which apply within the public sector, do generally not apply within the private sector unless your disclosure is protected under applicable law.

E. Belgium

Practical Guidance – Whistleblowing Protections

The Belgian Whistleblowing Act will only protect those who report a violation the following areas:

- Public procurement; financial services, products and markets, and prevention of money laundering and terrorist financing;
- Product safety and conformity;
- Transport safety;
- Environmental protection;
- 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 networks and information systems
- combating fiscal fraud;
- Combating social fraud.

In section 1.5 (How to report?) the following is changed:

✓ A Member of your senior local company management*

*Please consider if there is a conflict of interest when reporting to your senior local company management and if so, please report to another internal Speak Up Resource or our external Speak Up Channels.

In section 1.5 (How to report?) the following is added:

A report can be made in writing, orally or both. It is possible to report orally by phone or another voice recording system and, if requested by the whistleblower, in a face-to-face meeting within a reasonable time.

In section 1.8 (How do we handle your report?) – bullet 12 - the following is added:

Furthermore, personal data will be kept no longer than when the reported violation is time-barred.

Once we received your report, we strive to acknowledge this receipt within 7 days is changed to: Once we received your report, we will acknowledge this receipt within 7 days.

In section 1.9 (No retaliation) the following is added:

Any person who has made a report and who is a victim of or threatened with reprisals may submit a reasoned complaint to the Federal Ombudsman, who shall initiate an extrajudicial protection procedure. The complaint can be made by following the form accessible through the following link:
https://www.federaalombudsman.be/fr/formulaireplainterepr%C3%A9sailles.

F. Bulgaria

Practical Guidance – Whistleblowing Protections

To benefit from the whistle blower protection in compliance with the Bulgarian legislation, a Speak Up report must concern breaches of the Bulgarian and/or the EU law, committed not more than two years before the reporting, concerning any of the matters expressly stipulated by the applicable legislation, such as (without being limited to):

i. financial services, products and markets, and prevention of money laundering and terrorism financing;
ii. product safety and compliance;
iii. protection of the environment;
iv. food safety
v. public health;
vi. consumer protection;
vii. protection of privacy and personal data;
viii. security of network and information systems;
ix. breaches of the Bulgarian labour law.

In section 1.6. (Information to provide) the following is added:
When filing written reports, you should use the template form adopted by the Bulgarian Commission on Personal Data Protection available here:

Bulgarian version:
https://www.cpdp.bg/userfiles/file/ZZLPSPOIN/ZZLPSPOIN_Formuljar%20za%20Registrirane%20na%20Signal(1).docx

English version:
https://www.cpdp.bg/userfiles/file/ZZLPSPOIN/WPA_Report%20Registration%20Form%20for%20the%20Submission%20of%20Information%20on%20Breaches%20under%20the%20Whistleblower%20Protection%20Act_En.DOCX

Oral reports shall be documented by the completion of the same form by the person responsible for receiving your report. Where possible, that person will ask you to sign the form.

In section 1.7. (Anonymous Reporting) the following is added:
Anonymous reports of violations under the whistleblowing regulations will not be handled and investigated.

In case that a whistleblowing report has been submitted anonymously under other rules and subsequently the reporter has been identified and retaliated against, the reporter will be entitled to the whistle-blowers protection, provided that all other statutory requirements for this protection to apply are met.

G. Luxembourg

Practical Guidance – Whistleblowing Protections

The law in Luxembourg provides the protection of the law for all reports made for acts that are unlawful or are contrary to the object or purpose of directly applicable provisions of national law. However, reports about other topics are not forbidden. In addition, the Labour Code provides additional protection against reprisals to employee protesting or refusing to act for certain facts that constitute a breach of regulation.

In section 1.5 (How to report?) the following is added:

In addition to the internal and external Speak Up Resources above, Code of Conduct Committee Chair is hereby designated as the impartial person or service responsible for handling and following-up on reports for Luxembourg. You may file a report directly, in either Luxembourgish, French and German or any other language spoken within CCEP.

In section 1.7 (Anonymous reporting) the following is changed:

Please note that all our reports are handled in a safe and confidential manner as far as reasonably practicable unless this is not allowed or required by law and/or risks the investigation by national authorities or judicial proceedings is changed to: Please note that all our reports are handled in a safe and confidential manner unless this is not allowed or required by law and/or risks the investigation by national authorities or judicial proceedings.

In section 1.8 (How do we handle your report?) the is changed:

Once we received your report, we strive to acknowledge this receipt within 7 days is changed to: Once we received your report, we will acknowledge this receipt within 7 days.

In section 1.10 (Data protection) the following is changed and added:

Your identity and other non-public information you shared in relation to the report will be treated confidentially so far reasonably practicable is changed to: Your identity and other non-public information you shared in relation to the report will be treated confidentially.

The following is added after the paragraph ***Data privacy:***

Personal data which is clearly not relevant for the processing of a specific report shall not be collected or, if collected accidentally, shall be erased without undue delay. When we use a recording voice messaging system, with your prior consent, such recording shall be done by a recording of the conversation in a durable and retrievable form or by a full and accurate transcript of the conversation made by the person responsible for handling the report. You will have the right to verify, correct and approve the transcript by signing it.

H. Netherlands

Practical Guidance – Whistleblowing Protections

To benefit from whistleblower protection, a Speak Up report must concern in general:
a. A violation or a threat of violation of Union law, or
b. An act or omission in which the public interest is at stake

- A violation or a risk of violation of a legal provision or of internal rules that entail a specific obligation and which have been established by an employer on the basis of a legal provision;
- danger to public health, to the safety of persons, to damage to the environment or to the proper functioning of the public service or a company as a result of an improper act or omission;
- The public interest is in any case at stake if the act or omission does not only affect personal interests and there is either a pattern or structural character or the act or omission is serious or extensive

In section 1.5 (How to report?) the following is added:

A report can be made in writing, orally via phone or another voice recording system and, when requested within a reasonable time, in an on-site conversation. When a verbal report is made, CCEP will either record the conversation with your consent or will make a detailed transcript of the conversation. In case a transcript is made, you will have the opportunity to check, rectify and sign it.

Please note, if needed, you can consult a counsellor to confidentially discuss the suspected breach.

In section 1.8 (How do we handle your report?) the following is changed:

In certain limited circumstances, CCEP may need to disclose your identity. This may happen when certain obligations are imposed by law. In such cases, we will make sure to apply appropriate safeguards, and to share the disclosure with you in advance, explaining the

reasons that justify it, unless this is not allowed or required by law and/ or risks the investigation by national authorities or judicial proceedings is changed to: In certain limited circumstances, CCEP may need to disclose your identity. This may happen when certain obligations are imposed by law. In such cases, we will make sure to apply appropriate safeguards, and to share the disclosure with you in writing in advance, explaining the reasons that justify it, unless this is not allowed or required by law and/or risks the investigation by national authorities or judicial proceedings.

Once we received your report, we strive to acknowledge this receipt within 7 days is changed to: Once we received your report, we acknowledge receipt within 7 days.

We expect that within three months from the acknowledgement of receipt, we will be providing you with feedback in relation to your report where this is reasonably practicable is changed to: Within three months from the acknowledgment of receipt, we will be providing you with feedback in relation to your report and, if applicable, with any follow-up actions taken.

I. France

Annex – specific provisions applicable in France

The provisions presented below are complementary to the information detailed in these Guidelines.

Who can report?

In accordance with §1.2. Guidelines, anyone connected to CCEP by a current or past professional context can make a report.

This person must report without direct financial compensation and in good faith. Where the person making the report has not obtained this information in a professional context, he must have had personal knowledge of it.

What can be reported?

France provides for a large number of information that may be subject to a report:

- a crime, an offense: for example, in case of corruption, harassment, tax evasion…;
- A violation of the LOI, the Regulation, EU law or an act of an international organisation: For example, in the event of a violation of regulations on safety, health, human rights…;
- a threat or harm to the public interest;
- A violation of the CCEP Code of Conduct or its policies (including anti-corruption).

Alerts may relate to events that may or may have occurred.

How can a report be made?

The procedures for making a report are described in § 1.5. Guidelines.

In the event of an oral report, the author of the report may request to organize a videoconference or a physical meeting with CCEP. This exchange will be organized, as far as possible, within a maximum period of 20 working days after receipt of the request.

How are reports handled?

Reports are processed in accordance with § 1.8. Guidelines.

In France, reports are handled by the local Ethics Committee with the support and according to the needs of the People & Culture, Internal Audit, Legal and Security teams. In order to ensure their impartiality, such persons shall follow the applicable internal investigation procedure, ensure that there are no conflicts of interest and are specifically trained in the handling of alerts.

When other persons or services receive reports, they shall forward them without delay to the persons mentioned above.

What is the applicable protection?

The whistleblower can benefit from the various protections detailed in the guidelines and provided for by the LOI. In particular, they are protected against any retaliation (§ 1.9.).

Any report made in good faith, even if the facts prove to be inaccurate or unacted upon, cannot expose the perpetrator to punishment or reprisal.

On the other hand, abusive use of the speak Up device (for example in case of desire to harm) could expose its author to possible disciplinary sanctions as well as legal proceedings.

What is the information of the reporter?

The author of the report is regularly informed by CCEP about the receipt and processing of his report, under the conditions defined in § 1.8. Guidelines.

Where an alert is considered not to fall within the scope of these guidelines, the author of the alert shall also be informed. In this case, the report may be processed by CCEP or archived as appropriate.

The author of the alert shall be informed of the closure of the case.

What are the confidentiality guarantees?

These guidelines ensure strict confidentiality of the identity of the authors of the report, the persons targeted, and any third parties mentioned in the report. They shall also preserve the confidentiality of the information collected by all the addressees of the alert.

The information collected may only be disclosed to third parties if such disclosure is necessary to process the report. In addition, elements likely to identify the whistleblower may not be disclosed without his consent[1].

What are the safeguards for the protection of personal data?

Reports are processed in accordance with the applicable regulations on the protection of personal data and the internal policies of CCEP detailed in § 1.10. Guidelines.

Alerts shall be kept only for as long as is strictly necessary and proportionate for their processing and for the protection of their authors, the persons referred to and the third parties referred to therein, taking into account the time limits for any further investigations.

Data relating to alerts may, however, be retained beyond that period if the natural persons concerned are neither identified nor identifiable.

[1] By way of exception, these elements may be communicated to the judicial authority in certain cases.