Speak Up Procedure

25/11/2021

Introduction

Ontex's Code of Ethics provides **Employees** (as defined under point 1.1 below) and **those doing business on behalf of Ontex** (as defined under point 1.2.b below) with a clear set of legal and ethical business principles that they are expected to follow in their day-to-day work for Ontex. **Ontex** (meaning the Ontex group of companies, comprising Ontex Group NV and its subsidiaries) expects Employees and those doing business on behalf of Ontex to always act lawfully, ethically and with integrity, taking Ontex's Values into account.

Ontex believes that the true measure of success is not just the results Employees and those doing business on behalf of Ontex achieve, but how they achieve them. For this reason, there should be no gap between what they say and how they act. A crucial element to achieve this, is that Ontex is committed to establish an open culture where all people feel secure in seeking advice and raising concerns.

Ontex expects Employees and **Third parties** (as defined under point 1.2) to speak up if they believe, in good faith, that there is a violation or potential violation by Employees or those doing business on behalf of Ontex , of Ontex's Values, its Code of Ethics, its policies (referred to in the Code of Ethics) or the law (hereafter referred to as a "**Potential Incident**"). It may seem easier to keep silent or look the other way, but people speaking up (hereafter referred to as "**Reporters**") can provide Ontex with information about illegal or unethical behavior that may imply severe risks for Ontex and its stakeholders. Remaining silent about possible misconduct may worsen a situation, decrease trust and prevent remediation measures to be taken.

Ontex takes every Potential Incident seriously. Every Potential Incident will be investigated and in case a Potential Incident appears to be substantiated or partly substantiated (hereafter referred to as an "**Actual Incident**"), Ontex will take prompt corrective action and impose the necessary remediation measures to maintain a strong ethical business culture.

In order to enable the reporting of concerns through safe and reliable means and to ensure that all Potential Incidents are properly handled, Ontex has implemented a clear process, detailed in this **Speak up Procedure**, regarding the receipt, the assessment, the handling, the investigation, the remediation and the closure of Potential and Actual Incidents (both together hereafter referred to as "**Incidents**").

1. Who does Ontex expect to speak up?

1.1. Ontex employees

All Ontex employees (being individuals working at all levels and grades within Ontex including senior managers, officers, directors, permanent, fixed-term or temporary employees, trainees, seconded

staff, homeworkers, casual workers and agency staff, volunteers or interns, as well as consultants (with an Ontex email account), herein referred to as "**Employees**") are expected to speak up.

1.2. Third parties

Third parties professionally related to the business of Ontex, such as:

a. suppliers, customers, business partners, former employees or potential candidates, shareholders, as well as,
b. those doing business on behalf of Ontex (such as agents, distributors, joint venture partners, consultants (with no Ontex email account) and other third party intermediaries),

all herein referred to as "**Third parties**", are invited to raise concerns when facing Potential Incidents by Employees or those doing business on behalf of Ontex.

This Speak up Procedure applies to all Ontex locations, unless local deviations, documented in an annex to this Speak up Procedure, are required by law.

2. What concerns can be raised?

Employees and Third parties are encouraged to raise concerns and report behaviors, which they believe, in good faith, are Actuals Incidents.

Reporters must have reasonable grounds to believe that the information disclosed is an Actual Incident. Ontex will take disciplinary actions against Reporters who knowingly make a malicious allegation.

Employees and those doing business on behalf of Ontex against whom a concern is raised, as well as other individuals named in a Report, are hereafter referred to as "**Persons Concerned**".

3. How can a Potential Incident be raised?

3.1. Several internal channels

Ontex provides several internal channels for raising Potential Incidents. Employees and Third parties can report Potential Incidents to anyone they feel comfortable to speak to and in particular to:

- Specifically for Employees:
  - their **Line Manager** (meaning the Ontex employee they directly report to)
  - their **Local Person of Trust** (if such person has been appointed in their location)
  - their **Local Compliance Coordinator** (meaning the Employee(s) in charge of Compliance in a specific Ontex location. See list here)

- Other available channels:
  - **Group Compliance** (meaning the Employee(s) responsible for Compliance at Group level, via grpcompliance@ontexglobal.com)
  - **Internal Audit** (via internal.audit@ontexglobal.com) (meaning the Employee(s) responsible for Internal Audit within Ontex).

3.2. Speak up line

To report Potential Incidents, Ontex also provides a dedicated system (hereafter referred to as the "**Speak up line**"), operated by People Intouch B.V., based in The Netherlands, Amsterdam. Potential Incidents can be raised either through a web based portal (hereafter referred to as the "**Speak up web portal**") or by phone (hereafter referred to as the "**Speak up phone line**").

3.2.1. Speak up web portal

The Speak up web portal is available:
- For Employees: on Ontex Connect
- For Third parties: on www.ontex.com.

- Once they have accessed the portal, Reporters must first choose their **Ontex location** (being the list of countries where Ontex has a manufacturing plant or a sales office),
- then select their language
- and type or copy/paste their message.
- Once the 'send message' button is pressed, a screen with the case number and the message appears. A unique case number is attributed to the Potential Incident, which can be used by the Reporter anytime to check the status of the Potential Incident and/or add additional information.

The Speak up web portal has the advantage that the message can be printed out and documents can be uploaded.

3.2.2. Speak up phone line

The Speak up phone line is only available:
- For Employees
- in the Ontex locations listed in the list of countries published on Ontex Connect.

In other Ontex locations, Potential Incidents can only be reported via the Speak up web portal. The Speak up phone line is not accessible for Third parties.

- Potential Incidents can be reported via the Speak up phone line by dialling the local free phone number and entering the access code (see link on Ontex Connect for the list of phone numbers and for the access code).
- A message can be left after the beep tone.
- The Reporter receives a six digit case number, which is randomly generated. It is important to write it down as this case number will enable the Reporter to listen to Ontex's response when calling back later.

3.3. Anonymous report

In all cases, Reporters can share their concerns anonymously (unless this is not allowed by the laws of their country, in which case a specific annex is added to this Speak up Procedure). Ontex does however encourage Reporters to reveal their identity as it is more difficult, and in some circumstances even impossible, to investigate reports that are made anonymously.

3.4. Report in own language

In all cases, Potential Incidents can be reported in the Reporter's native language. Answers by Ontex to Potential Incidents reported via the Speak up line will be automatically translated in the language of the report.

3.5. External channels

Although Reporters are encouraged to use the internal channels provided for by Ontex under point 3.1 to 3.4 above, Potential Incidents can also be raised externally via the specific channel(s) made available by local authorities.

4. How does Ontex handle Incidents?

Introduction: Ontex's Case Management System

To handle and manage Incidents, Ontex uses a Case Management System (hereafter referred to as the "**CMS**"). The CMS contains a database of all reported Incidents.

4.1. Roles and access rights

The following 6 roles have been created in the CMS for the handling of Incidents. Each role (hereafter referred to as a "**Role**") has defined access rights and permissions to the Incidents. Except for Group Compliance who manages the CMS and has access to all Incidents registered in the CMS, all other Roles only have access to the Incidents they are involved in or informed of and this access is limited to what they need to know to perform their Role in the handling of the related Incident.

- Group Compliance: manages the CMS and has read and edit access rights to all Incidents registered in the CMS;
- Global Internal Audit Manager: has read access rights to all Incidents registered in the CMS;
- Local Compliance Coordinators: register new Potential Incidents for their Ontex Location and have read and edit access rights to the Incidents they have registered and/or for which they are appointed as Evaluators or Handlers;

- Evaluators: have read and edit access rights to Incidents for which they are appointed as Evaluators (see point 4.2.3 below);
- Handlers: have read and edit access rights to Incidents for which they are appointed as Handlers (see point 4.2.5 below);
- Investigators: have read and edit access rights to Incidents for which they are appointed as Investigators (see point 4.2.6 below).

To guarantee the highest level of information security and data privacy, data regarding Incidents are, to the maximum possible extent, kept solely in the CMS and communication between the above mentioned Roles, takes place within the CMS.

4.2. Handling of Incidents

Reported Incidents are handled as follows[1]:

4.2.1. Registration in CMS and good receipt

- Potential Incidents reported via the internal channels (see point 3.1) are sent to Group Compliance or to the Local Compliance Coordinators by the Reporters or by those to whom a Potential Incident was reported.

  Group Compliance or the Local Compliance Coordinator registers the Potential Incident in the CMS and sends a good receipt to the Reporter within 3 working days after being informed of the Potential Incident.

- Potential Incidents reported via the Speak up line (see point 3.2) are automatically registered in the CMS. Group Compliance receives a notification of those reports and acknowledges good receipt thereof within 3 working days.

4.2.2. Qualification as Potential Incident

Group Compliance first checks if the reported concern qualifies as a "Potential Incident". If the reported concern does not qualify as a Potential Incident, the Reporter is asked to contact the relevant department and the Potential Incident is mentioned in the CMS as a 'non-Incident'.

When the Potential Incident qualifies as a 'non-Incident', Personal Data (as defined under point 7 below) relating to that 'non-Incident' will be anonymized.

Reports that qualify as Potential Incidents are further handled as described below.

4.2.3. Classification of the Potential Incident

[1] Depending on the circumstances, Group Compliance may decide to deviate from this process to ensure the proper handling of a Potential Incident.

Group Compliance classifies the Potential Incident as yellow, orange or red depending on criteria, such as the type of the Potential Incident or the Persons Concerned involved.

This classification determines who is appointed as "**Evaluator(s)**", in line with the "Code of Ethics Incidents Escalation Process". The tasks of the Evaluators are further described under points 4.2.4, 4.2.6 and 4.2.7.

4.2.4. Assessment of the Potential Incident by the Evaluator(s)

Based on the information given in the report, including the type of Potential Incident, the Evaluators appoint a "Handler" (see point 4.2.5).

4.2.5. Handling of the Potential Incident

Once appointed by the Evaluator(s) the Handler:

- Investigates the Potential Incident;
- If additional information is necessary to proceed with the handling of the Potential Incident, requests such information from the Reporter;
- Reports to the Evaluator(s) on the findings and outcome of the investigation.

4.2.6. Specific investigation of the Potential Incident

- In case specific investigation is needed, the Evaluator(s) can decide to assign an Investigator, such as the Global Internal Audit Manager (or his team) or an external expert (lawyer or other consultant) to investigate the entire or some specific parts of the Potential Incident.
- The Investigator reports on the findings and outcome of the investigation to the Evaluator(s).

4.2.7. Measures and next steps

Based on the findings and outcome of the investigation shared by the Handler and/or the Investigator, the Evaluator(s) decide whether the Potential Incident is an Actual Incident and if so, decide upon follow-up measures, next steps and potential sanctions.

4.2.8. Feedback to the Reporter

The Reporter is informed about the status and the outcome of the investigation within the timing mentioned under point 5.4. below.

4.2.9. Closure of the case

Once all the above steps are taken, and the Reporter has taken notice of Ontex's feedback, Group Compliance closes the Incident in the CMS.

5. How do handling/investigations take place?

5.1. Conduct of investigations

An investigation is, in first instance, a fact-finding exercise to determine whether an Actual Incident has taken place.

All investigatory measures which are deemed necessary for the proper handling of a Potential Incident will be taken, in line with applicable laws.

5.2. Independence of investigations

5.2.1. Handlers and Investigators have the duty to determine in all objectivity and independence whether the Potential Incident is substantiated and will therefore conduct the investigation with integrity, fairness and diligence, free from actual or apparent bias or conflict of interest and in a professional and impartial way. They will not be put under any kind of pressure, will be given the necessary time to conduct the investigation and will operate independently.

Any attempt to influence or put pressure on a Handler or Investigator may lead to disciplinary action.

5.2.2. All Employees and those doing business on behalf of Ontex are expected to cooperate fully with any Handler and/or Investigator and to provide complete and truthful information. Employees who have been informed or become aware of ongoing investigations for which they have relevant records (e.g. memoranda, electronic mail, instant messages, files, notes, photographs, recordings, etc.) must provide these records to the Handler and/or the Investigator.

5.2.3. In case any of the Roles mentioned under point 4.1 qualify as Persons Concerned, they will not be involved in the handling of that Potential Incident, nor informed of that Potential Incident (except if this is absolutely necessary for the sake of the investigation).

5.3. Confidentiality of investigations

5.3.1. Maintaining confidentiality is critical to guarantee the integrity of an investigation. Every aspect of an investigation, including the identity of the Reporter and/or of any person named in the report of a Potential Incident and/or any information which is likely to lead to their identification and/or details of the Potential Incident and of the investigation, is kept strictly confidential and is disclosed on a need-to-know basis only, to those who are involved in the handling of the concerned Incident.

5.3.2. Ontex reserves the right to refer any concerns or Incidents to appropriate external regulatory or judicial authorities.

5.3.3. Ontex keeps the Reporter informed of the progress and outcome of the investigation. However, the need for confidentiality and legal considerations may prevent Ontex from providing the Reporter details on the investigation, on its outcome or on disciplinary actions taken.

5.3.4. An internal reporting of Incidents to Ontex's Executive Management Committee or Board of Directors takes place regularly where details of investigations and Incidents may be disclosed. Details of investigations and Incidents may also be disclosed to Ontex's external auditor.

5.4. Timing of investigations

5.4.1. Ontex expects each Role to give priority to the handling of Incidents when an assignment or request is directed to them in the CMS. The investigation needs to be done promptly in order to stop Actual Incidents as quickly as possible and to take corrective actions when needed.

5.4.2. Ontex aims to investigate Potential Incidents within maximum three (3) months from the date on which the concern was raised by the Reporter. The Reporter is informed of the outcome of the investigation. If the investigation is still ongoing after three (3) months, the Reporter is informed of a new timeframe within which Ontex expects to provide a new update.

5.4.3. If after a request was sent to the Reporter (for example, to obtain additional information) or after the Reporter was informed of the outcome of the investigation, the Reporter does not log on the Speak up web portal or call back on the Speak up phone line for more than one (1) month, Ontex will close the Incident and the case will not be accessible to the Reporter anymore thereafter.

6. Non-retaliation

No single Reporter shall be discharged, suspended, threatened, harassed, intimidated, coerced or retaliated against in any other manner as a result of him or her reporting a Potential Incident, making a good faith notification, asking for advice about a specific matter, action or decision or cooperating in an investigation following the reporting of a Potential Incident.

This non-retaliation principle will be applied even if the notification is proven to be unfounded after investigation, unless the person raising the concern knowingly made a false allegation, provided false or misleading information in the course of the investigation, or otherwise acted in bad faith.

Retaliation against a Reporter is taken very seriously. Complaints on potential retaliation will be reviewed promptly and investigated and adequate disciplinary measures will be taken against those who retaliate.

7. Protection of Personal Data

The handling of an Incident inevitably leads to the processing of personal data (herein referred to as "**Personal Data**") in the sense of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the transfer of such data internally (so-called "**GDPR**") and all other applicable privacy laws. Without prejudice to local legal requirements, Ontex BV, a company registered under Belgian law having its registered offices at Genthof 5, 9255 Buggenhout, Belgium, company number 0419.457.296, qualifies as data controller (in the sense of the GDPR) in relation to Incidents registered in the CMS. The legitimate interests of the data controller to detect and deal with Incidents clearly justify the processing of personal data. It will ensure that every processing of Personal Data in this respect is done in compliance with the GDPR and all other applicable privacy laws.

The Speak up line is operated by People Intouch BV, which qualifies as data processor (in the sense of the GDPR), under a contract that complies with applicable data privacy legislation, and which – amongst other provisions – provides for the following technical and organizational measures for protection of Personal Data to be implemented:

- Access Controls Policy;
- Physical & environmental security;
- Operations security management;
- Software development and maintenance;
- Business Continuity management;
- Incident management;
- Information security suppliers;
- Compliance asset management.

The processed data may also be transferred to third parties, such as the police, financial or other authorities, auditors or external advisors, that would be called upon in the framework of the handling of a Potential Incident. Within Ontex, the Personal Data will only be accessible to the relevant functions and only to the extent that such access is required for the correct application of the Speak up Procedure.

Every processing will be documented and unproven or irrelevant data will be discarded. In any event, personal data will not be stored beyond the relevant statute of limitation applying to the facts under review.

Reporters will be entitled to access and correct the Personal Data relating to them. Data of other data subjects are not accessible. Personal Data that would be incomplete, no longer required or accurate,

will be deleted. These rights can be exercised by contacting the Group Data Protection Officer ("DPO") on gdpr@ontexglobal.com. This right may however be restricted or postponed in the interest of an investigation.

The data subject acknowledges having been informed on the following rights, insofar as applicable:

- The right to request the data controller (through the Group DPO) to limit the processing regarding him/her, the right to object against the processing and the right of data transferability;
- The right to file a claim with the data protection authority.

8. Record keeping

Ontex shall keep records of every Potential Incident received in compliance with the above confidentiality measures. Ontex shall keep information on Incidents not longer than necessary and proportionate. The record keeping is held in the CMS.

Document information

Content owner:	Group Compliance
Email:	grpcompliance@ontexglobal.com
Classification:	Compliance
Revision:	04
Status:	Final
Approved by:	EVP Legal
Location:	Group
Business Domain:	all Ontex' Representatives
Date:	25-11-2021