Procedure for the Covéa whistleblowing system

2020 version

COMMITED
MUTUAL
INSURANCE
GROUP

Contents

INTRODUCTION

The Sapin II Law and the Law on the duty of care[1] require large corporations to implement a procedure for collecting whistleblower reports. The Sapin II Law also introduced a regime to protect whistleblowers.

Whistleblowing is intended to report serious occurrences, breaches of the Covéa Anti-Corruption Code of Conduct, and violations in relation to human rights and fundamental freedoms, the health and safety of persons, or the environment.

In accordance with these regulations, the Covéa Group has put a system in place to collect whistleblower reports.

This system enables everyone to be an active part of risk prevention.

It can be used by:

- anyone working for the Covéa Group (in-house staff or external, temporary or occasional staff), including persons belonging to another company that has set up its own whistleblowing system;
- any third party, for reporting violations in connection of the duty of care, as defined below, in relation to the activities of the Covéa Group and those of its subcontractors and suppliers.

The Covéa Group has taken all necessary steps to ensure that the identity of whistleblowers, personal data and any information transmitted in connection with whistleblowing remains confidential.

The system is based on the principles of good faith, fairness and respect for the right to defence.

It has been presented to the Employee Representative Bodies in accordance with the provisions of the law.

PART 1 – GENERAL PRINCIPLES

Scope of the system

Whistleblower alerts must relate to misconduct or situations that potentially constitute a breach of the rules applicable to the Covéa Group. This means :

[1] Currently: Law no. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life and Law no. 2017-399 of 27 March 2017 on the duty of care of parent companies and subcontracting firms

- Any **serious occurrence** such as:
  - a crime or other offence, including acts of corruption or influence peddling;
  - a serious and manifest breach of the law or statutory regulations (decrees, orders, regulations, etc.);
  - a serious and manifest breach of an international commitment duly ratified or approved by France;
  - a threat or serious harm to the public interest of which the whistleblower is personally aware,
- Any **conduct or situation** that may be **contrary to Covéa's Anti-Corruption Code of Conduct**,[2]
- Any risk of actual or potential **negative impacts related to the Group's activities or its business relationships**, pursuant to the Law on the duty of care[3].

	General provisions on whistleblowers	**Anti-corruption system**	**Whistleblowing mechanism under the duty of care**
Legal basis	Arts. 6 et seq. of the Law of 9 December 2016 ("Sapin II")	Art. 17-II of the Law of 9 December 2016 ("Sapin II")	Law of 27 March 2017 on the duty of care
Scope	- **Crime or other offence** - **Serious or manifest breach** • of an international commitment approved by France • of a commitment made on the basis of a unilateral act of an international organisation • of the law or regulations - A **threat or serious harm** to **the public interest**	**Any conduct or** situation that appears **contrary to the Covéa Anti-Corruption Code of Conduct**[4]	**Risk or occurrence of serious harm** to: • human rights • fundamental freedoms • the health and safety of persons • the environment … related to the activities or business relationships of the group and **arising from activities of the company, of companies it controls, or its subcontractors**

The range of matters that may be reported is wide.

[2] Covéa Anti-Corruption Code of Conduct, as appended to the Internal Regulations

[3] Law no. 2017-399 of 27 March 2017 on the duty of care of parent companies and subcontracting firms

[4] Covéa Anti-Corruption Code of Conduct, as appended to the Internal Regulations

A few examples are listed below:

- **Business and financial matters:**
  - Fraud, theft, embezzlement, misuse of corporate assets;
  - Money laundering, tax fraud, insider trading;
  - Abuse of a dominant position;
  - Non-compliance with the Anti-Corruption Code of Conduct: corruption, influence peddling, breaches of the rules on gifts and invitations.

- **Health, environment, safety and the protection of persons:**
  - Serious data protection breaches: large-scale data leak
  - Serious violations of individual rights and protections: discrimination, psychological or physical harassment, forced labour, violation of the freedom to join a trade union
  - Serious environmental breaches giving rise to a major risk or serious damage: pollution.

Exclusion: Facts, information and documents covered by medical secrecy, legal professional privilege or national defence secrecy are excluded from the scope of this provision.

Who can use the system

- **Covéa Group employees**

The whistleblowing system is an additional channel that is not intended to replace other existing channels (line management, employee representative bodies, public authorities) that the law provides for raising the alarm. Use of the whistleblowing system is optional.

If you know of a matter that is potentially the subject of a whistleblower alert, you may first bring it to the attention of your direct or indirect line manager, unless this person is involved in the misconduct or the facts in question.

If an employee approaches their line manager, the manager's role is to provide guidance and advice to the employee. If the manager feels that the matters fall within the scope of the whistleblowing system, they should encourage the employee to report them to the Contact Person via the system.

The whistleblowing system also offers enhanced safeguards to protect the whistleblower (in particular, all dealings with the Contact Person are confidential).

- **Third parties**

The whistleblowing system can also be used by third parties (individuals and legal entities)[5] in accordance with their duty of care.

Stakeholders in the system

Stakeholders	Features
Contact Person	The Contact Person is the person designated within the group to collect and process whistleblower reports[6]. At Covéa, this is the Covéa Compliance Director. The Compliance Director ensures the proper functioning of the entire whistleblowing system and chairs the Covéa Ethics Committee.
Reporting person	Anyone working for the Covéa Group – without exception – has access to the whistleblowing system, including external or occasional staff (temporary staff, interns, service providers). Any third party Note: An individual who makes a report is a "whistleblower", provided that they meet certain conditions. A legal entity which makes a report does not benefit from any particular protection in this regard.
Whistleblower	Whistleblowers enjoy protection under the law and their identity is strictly confidential (cf. section below on "Protection of whistleblowers"). A legal entity which raises an alert is not a whistleblower.
Line manager	A line manager who is contacted by an employee in relation to a whistleblower alert must provide guidance and advice to the employee.
Person concerned	Persons concerned by an alert benefit from the presumption of innocence. Their identity is kept confidential during the investigation.
Ethics Committee	The Ethics Committee is responsible for examining whether an alert is admissible and for overseeing the investigation of admissible alerts. It is made up of a limited number of members: the Chief Compliance Officer, the Head of Permanent International Control, the Head of Internal Audit. If so, depending on the object and context of the alert: the Head of Human Ressources, the Hard of Legal, the Head of Corporate Societal Commitment.
Investigation Unit	The Investigation Unit is responsible for investigating alerts. Its members, the number of whom is restricted, are appointed by the Ethics Committee. If necessary, they may be joined by persons with additional skills.

[5] For example: trade unions, non-governmental organisations, victims' associations, local authorities etc.

[6] Pursuant to Article 4 of Decree No. 2017-564 of 19 April 2017 on procedures for collecting reports by whistleblowers

Protection of whistleblowers

Anyone making a report has "whistleblower" status if they meet the following conditions:

- **they are a private individual** (i.e. not a legal entity), regardless of the nature of their relationship with the Covéa Group (professional/non-professional).
- **they have personal knowledge of the reported facts:** the whistleblowing system should not be used to report matters you have only heard about from a third party.
- **they act disinterestedly,** i.e. they act in the public interest and will not obtain any personal benefit from what they do.
- **they act in good faith:** they must state the facts objectively and without malice. The presumption is that the reporting person is able to draw up or produce information as objectively as possible. Any information provided must be directly related to the scope of the whistleblowing system and be strictly necessary for the verification of the alleged facts. It should be worded in a way that makes clear what you believe the nature of the matters reported to be.
- **they report serious matters** as defined above.

If the above conditions are met, the whistleblower enjoys legal protection, as follows:

1. Guaranteed confidentiality

The system guarantees that the whistleblower's identity, the identity of the person concerned by the report person, and the information gathered at all stages of the handling of the alert will be kept confidential**.**
This means that:

- The contents of an online whistleblower alert are encrypted[7] and password-protected.
- All contact between the whistleblower and the Contact Person via the secure platform[8] is confidential.
- Whistleblower alerts, as well as the investigations into them and any ensuing reports, are dealt with in complete confidentiality.
- The number of persons dealing with whistleblower reports (Contact Person, Ethics Committee members, Investigation Unit) is restricted and all of them are subject to a strict duty of confidentiality.
- Any experts engaged in connection with the inquiry will be contractually bound to keep data relating to the whistleblower alert confidential and to delete such data at the end of their investigations.
- Information that could identify the whistleblower may not
  - be disclosed under any circumstances to the person concerned by the alert, even if they exercise their right of access under data protection law
  - be disclosed to anyone except the judicial authorities without the whistleblower's prior consent.

[7] AES encryption algorithm
[8] Compliant with ISO 27001: Information Security Management and ISO 27018: Code of Practice for Protection of Personally Identifiable Information

2. Protection under criminal law

The whistleblower's identity details are confidential and disclosing them is punishable as a criminal offence[9].
Any person who tries to prevent a whistleblower from raising an alert may be punished for the offence of preventing the submission of an alert[10].

Whistleblowers cannot be held criminally liable for disclosing a secret protected by law, provided that all of the following conditions are met:

- Disclosure of the information is necessary and proportionate to the safeguarding of the interests in question;
- The report is made in compliance with this present procedure and is within the scope of the whistleblowing system;
- The reporting person qualifies as a whistleblower.

3. Protection under employment law

In accordance with the law, the Covéa Group guarantees that whistleblower reports will not lead to disciplinary measures or prosecution in the circumstances set out above.

Whistleblowers are therefore protected against all direct or indirect discriminatory measures, including discrimination with regard to pay or career development, and they will not face any disciplinary sanctions or reprisals for having raised an alert in accordance with this procedure.

Misuse of the system

Use of the whistleblowing system requires everyone to act responsibly.

Whistleblowers must act in good faith. They must not deliberately make false accusations or make reports with the sole intention of harming others or obtaining personal gain.

Anyone using the whistleblowing system abusively or in bad faith may be subject to disciplinary sanctions (if they are an employee) and could potentially be sued (for defamation or malicious false accusation).

Examples:

- *reporting allegations that the reporting person knows to be false*
- *acting in bad faith or abuse of law*

[9] Penalties: prison sentence of 2 years and fine of €30,000
[10] Penalties: prison sentence of 1 year and fine of €15,000

Compliance with the French Data Protection Act

Because the system put in place by Covéa requires the processing of personal data, it must comply with data protection regulations. The CNIL (French Data Protection Authority) has established a reference framework[11] for whistleblowing procedures that ensures their compliance with data protection rules.

[11] Ruling No. 2019-139 of 18 July 2019 adopting a framework related to the processing of personal data intended for the implementation of a professional whistleblowing system.

PART 2 – REPORTING AN ALERT

Access to the online reporting platform

Protecting whistleblowers is a fundamental concern for the Covéa Group, which has selected the WhistleB secure platform to collect and manage all communications and information relating to reports.

This external platform is available:

- 7 days a week, 365 days a year,
- from all countries,
- in French, English and Italian.

It can be accessed from any Internet-connected device (computer, tablet, smartphone).

Access is secure and the content is encrypted (see Section on "Confidentiality guarantees"). The data is hosted on an external server that is not connected to the Covéa Group's IT systems.

To make a report in the whistleblowing system, you must go to the WhistleB platform:

- For employees : https:/report.whistleb.com/covea
- For third parties : www.https://report.whistleb.com/fr/covea-vigilance

This website address is publicised internally and externally.

Making a report

Anyone can use the whistleblowing system to report matters that fall within the scope of this procedure.

Whistleblowers should state their identity by completing the online form.

Identifying yourself has a number of benefits:

- it allows you to be protected effectively;
- it allows the report to be processed more effectively, by making it possible to contact you for additional information.

Anonymous alerts can only be acted on if the matters reported are serious and described in sufficient detail. The Contact Person must ensure that extra precautions are taken when handling an anonymous alert, particularly when checking whether it is admissible.

Users of the system are thus encouraged to state their identity when they make their report, with a guarantee that any data that could potentially identify them will remain confidential.

Anyone making a report must:

- indicate the facts of the matter reported, giving enough information to identify the situation and, if possible, the persons involved;
- attach documents to the report, where appropriate;
- confirm that they have read and acknowledged this procedure before finalising their report;
- submit their report.

Confirmation of receipt

Once the alert has been sent, the platform immediately displays a dated confirmation of receipt. This will:

- confirm that the report has been recorded on the platform;
- state the expected time required to check whether the report is admissible;
- provide a set of login details (username and password), which the reporting person will need to log on to the platform in order to track the progress of the report. Doing this allows you to:
  - provide additional information about their alert during the investigation, if needed;
  - stay informed about what action is being taken.

The confirmation of receipt is displayed in the language used by the whistleblower (French, English, Italian).

Information for platform users

The Covéa whistleblowing system, which collects and processes reports, involves the automated processing of personal data.

Reports must relate to breaches of Covéa's Anti-Corruption Code of Conduct or to another risk or serious occurrence as defined in the "Scope of whistleblower alerts" paragraph of this procedure.

Use of the system is optional. Therefore, employees cannot be punished for failing to use it.

Special security measures *(see section on "Confidentiality guarantees")* are taken by the data controller to preserve the confidentiality of whistleblowers' identities and maintain data security.

Data about whistleblowers is passed to the authorised persons in charge of collecting and managing alerts within the Covéa Group (Contact Person, Ethics Committee and Investigation Unit).

Under no circumstances will this data be communicated to the persons concerned by the alert, even if they exercise their legal right of access.

Data collected by the whistleblowing system may be passed to experts engaged to assist with inquiries, solely for the purposes of those inquiries. Any such experts will be contractually bound to maintain confidentiality.

Whistleblowers, as private individuals, have the right of access, rectification and deletion of their data, which they can exercise by contacting the Contact Person via the secure platform. The Contact Person will process such requests in conjunction with the Data Protection Officer.

PART 3 – PROCESSING AN ALERT

Checking that an alert is admissible

Whenever a report is received, it will first be checked to ensure that it is admissible. This involves checking that:

- the report is within the scope of this procedure;
- the information reported is factual and is detailed enough to be verified.

This check is performed by the Contact Person and at least three of the five members of the Ethics Committee meeting face to face or remotely.

The decision taken is recorded in the alert management system (the WhistleB platform).

The whistleblower[12] can view this decision by logging on to the platform.

In all cases, the whistleblower will be informed of the admissibility of their report via the secure platform.

The **maximum** period for checking the **admissibility** of an alert must not exceed 30 calendar days.

Once the check is complete:

- Inadmissible reports are classified as "no further action" and retained in an anonymised form for six years[13], for evidential purposes in case a subsequent dispute arises.
- Admissible reports are investigated as appropriate. Admissible reports are described as "alerts".

Rights of persons concerned by alerts

For alerts declared **inadmissible**:

- Employees are informed that their personal data has been processed in connection with the alert system for the Anti-Corruption Code of Conduct, as appended to the Covéa internal regulations. This general notice is also assured by this procedure, which is available on the company intranet.
- Where the person concerned by the alert is a legal entity (the Covéa Group, a subsidiary, a sub-contractor or supplier), there is no similar obligation to provide information under the duty of care.

[12] Or the reporting person, if the report is made by a legal entity in connection with its legal duty of care

[13] Duration of the statute of limitations for criminal offences; see Article 8 of the French Criminal Procedure Code

For alerts declared **admissible**:

An individual concerned by an admissible alert will be informed of the existence of a procedure that involves the recording of their personal data by the Contact Person.

They will be informed in writing by any appropriate medium (letter, email) of:

- the entity in charge of the system;
- the purposes of processing and the legal grounds for processing;
- the fact that data about them has been recorded and, more specifically, the allegations made against them;
- the recipients of this information;
- the data retention period;
- how to exercise their rights to access, rectify and delete data.

However, the provision of this information may be delayed if it is likely to seriously compromise the achievement of the aims of the data processing. Persons concerned by an admissible report will therefore not be informed about it until precautions have been taken to prevent the destruction of evidence about the matters reported.

Information that allows the identity of a person concerned by a report to be ascertained cannot be disclosed, other than to the judicial authorities, until an investigation has been conducted to establish the facts.

Anyone concerned by an alert is presumed innocent until the allegations against them have been proved.

As data subjects, persons concerned by an alert have a right of access, rectification and objection, which they can exercise by contacting the Contact Person.

- The right of access cannot be used to obtain details of the whistleblower's identity, data relating to third parties or information collected during inquiries.
- If exercising the right of access would compromise the effectiveness of an internal investigation, the Contact Person may delay their response for the time necessary to preserve the evidence.
- As data subjects, persons concerned by a report may also exercise their right of rectification where the data concerning them is inaccurate, incomplete, ambiguous or out of date.
- Data subjects may not object in principle to the processing of data, as the whistleblowing system represents a legal obligation on the part of the data controller. They can only request the deletion of erroneous or inaccurate data.

Investigation of the alert

Where an alert is deemed admissible, the investigation of it is overseen by the Ethics Committee.

The Committee may instruct the Investigation Unit, whose role is to investigate the matters reported in order to establish whether they can be proved.

The Investigation Unit may contact the whistleblower via the secure platform to obtain additional information it needs to examine the alert.

Whistleblowers can use the secure platform to provide new information (including attachments) in support of their alert of their own volition at any time.

All necessary precautions will be taken to preserve evidence that allows the facts to be established.

The persons appointed to conduct the inquiries will draw up a report on their work and present it to the Covéa Ethics Committee.

After examining the case, the Ethics Committee may decide to:

1. classify it as "no further action", if the facts are not proved,
2. entrust the case to the competent department, if the facts are proved.

After it has examined the case file, the department engaged by the Ethics Committee will inform the Committee in writing as soon as possible of the final decision made and the action to be taken.

Cases are to be processed in a period of 90 calendar days.

If this deadline is exceeded, the Ethics Committee will keep the whistleblower/person making the alert informed about the progress of the case via the secure platform.

Closure of the alert

The whistleblower/reporting person and the person concerned by the alert will be informed of the closure of the whistleblowing procedure and the decision reached at the end of the investigation of the case, regardless of its outcome.

- Whistleblowers will be informed via the secure alert platform.
- The person concerned by the alert will be informed by any appropriate medium by the Contact Person or a member of the Ethics Committee. If allegations are made against an employee, they will be informed by the Human Resources Department according to the existing process.

Retention and deletion of collected data

Situation	Retention period
Report deemed inadmissible	• Promptly anonymised • Retained for six years in intermediate archiving (restricted access)
Alert classified as "no further action" after investigation	• Promptly anonymised (within 2 months of the closure of the investigations) • Retained for six years in intermediate archiving (restricted access)
Reported facts are proved but do not give rise to disciplinary or legal proceedings	• Promptly anonymised • Retained for six years in intermediate archiving (restricted access)
Reported facts are proved and give rise to disciplinary or legal proceedings	• Data retained until the end of the proceedings and any appeals • File is anonymised

Data is stored in the alert management system, access to which is limited to authorised persons only (Contact Person, Investigation Unit).

Strict confidentiality of the data is ensured by double authentication throughout the storage period.

PART 4 – ESCALATION PROCEDURE

To benefit from the protection afforded to whistleblowers, a reporting person must in all cases comply with the three-stage procedure provided for by law, as follows:

- **Level one:** the issue should be reported to the organisation itself, in accordance with the procedure described above.
- **Level two:** if the report is not acted on internally within a reasonable period (90 calendar days for Covéa), the issue must be reported to the competent judicial or administrative authorities, or to the National Contact Point where the legal duty of care applies[14]
- **Level three:** as a last resort, if the competent authorities fail to act on the report, it may be made public.

PART 5 – ALERT PROCEDURE IN INSURANCE OR BANKING

Covéa Group employees who, in the course of their duties, witness breaches of the regulations on insurance or banking business[15] may report them in writing to the competent supervisory authority, which is either:

- the French Prudential Supervision and Resolution Authority (ACPR), or
- the French Financial Markets Authority (AMF).

In accordance with the regulations[16], these authorities have systems for receiving and processing whistleblower reports under conditions that ensure that the persons making the reports are protected, in.

[14] The French National Contact Point for the implementation of the guidelines of the Organisation for Economic Cooperation and Development (OECD) is responsible for promoting the OECD guidelines and responding to referrals for non-compliance with those guidelines.

[15] European law, the French Monetary and Financial Code, the General Regulation of the French Financial Markets Authority

[16] Article 16 of Law No. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of the economy

PART 6 – EMERGENCY PROCEDURE

In the event of serious and imminent danger or a risk of irreversible damage, whistleblowers may report issues directly to a judicial or administrative authority.

They may also make them public.

Whistleblowers must use this option carefully and responsibly, as they will risk prosecution if they exercise it in the absence of an incontestable emergency.

Note: the law[17] entrusts the Ombudsman (Défenseur des Droits) with the task of providing guidance on taking this step to whistleblowers. The Ombudsman has published a guide (in French) on the guidance and protection of whistleblowers, which can be consulted via the following link:

https://www.defenseurdesdroits.fr/fr/guides/orientation-et-protection-des-lanceurs-dalerte

[17] Article 8 of Law no. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of the economy

The Covéa Whistleblowing Procedure is available on the Covéa intranet and on the website http://www.covea.eu

Covéa

Mutual Group Insurance Company governed by the French Insurance Code
RCS Paris 450 527 916
86-90 rue Saint Lazare
75009 Paris

Follow @groupecovea

www.covea.eu