PROCEDURE

The Covéa Internal Whistleblowing System

November 2023

Our commitment

Whistleblowing is a right enshrined in the French Sapin 2 Act that plays a part in preventing risks and promoting business integrity.

At the Covéa Group, we make every effort to comply with the various regulations that govern our activities, we prohibit all forms of bribery and influence-peddling in the conduct of our business and we take action to prevent violations of human rights and fundamental freedoms, harm to human health and safety and adverse impacts on the environment.

Thanks to the Covéa internal whistleblowing system, all our internal and external stakeholders, particularly our employees and business partners, can safely report potential breaches of regulations or unethical conduct.

The system we have in place is an effective way to detect situations that may present a risk to the company and to build further on our culture of integrity.

At the Covéa Group, we provide assurances that all whistleblowing reports will be handled in the strictest confidence and that informants who act in good faith will be protected from any retaliation measures.

For this whistleblowing system to work, it must be widely circulated and truly understood by the people who may one day need to use it. That is why we have published this procedure, which we have communicated on our intranet site and on our corporate website www.covea.com.
The Covéa internal whistleblowing system is also referred to in the Covéa Group's ethics charter and anti-bribery code of conduct.

I know that I can count on all Covéa staff to use this whistleblowing system responsibly, so that we can identify areas in which we can improve as a Group.

Thierry DEREZ
Chief Executive Officer

CONTENTS

PRELIMINARY REMARKS

LEGAL FRAMEWORK

1. The Covéa internal whistleblowing system is based on the principles and obligations arising from the French **Sapin 2 Act**[1] which introduced **protective measures for whistleblowers.**

2. The 21 March 2022 Waserman Act and its implementing decree[2] introduced additional protection through the following main amendments:

- any external stakeholder can now file a whistleblowing report with the company (e.g. a job applicant, former employee, subcontractor, supplier, customer, etc.);
- reports can now be filed directly with the competent authority;
- whistleblowers are now more protected, particularly against retaliation measures, and new protection measures have been introduced for anyone who helps them;
- a person may now report an issue even if they do not have personal knowledge of it, as long as they obtained the information in a work-related context.

This whistleblowing procedure reflects these amendments.

3. The Covéa internal whistleblowing system also fulfils the obligation to implement:

- a system for reporting any conduct or situation that is contrary to Covéa's anti-bribery code of conduct, under the **anti-bribery system**[3]**,**
- an alert mechanism to report any risk of actual or potentially negative repercussions associated with the Group's activities or its business relationships, under a **duty of care**[4] requirement.

---

1. French law No. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life (Art. 6 et seq.).
2. French decree No. 2022-1284 of 3 October 2022 on procedures for collecting and processing whistleblowing reports and establishing a list of external authorities provided for by the law (No. 222-401) of 21 March 2022 aimed at improving protection for whistleblowers.
3. French Law No. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life (Art. 17-II 3 et seq.).
4. French law No. 2017-399 on the duty of care of parent companies and contracting undertakings, which aims to prevent serious violations of human rights and fundamental freedoms, and serious harm to personal health and safety and the environment.

4. The internal whistleblowing system enables eligible individuals to report to the Covéa Group any issue that falls within the system's scope of application and ensures that all reports received are handled effectively and in the strictest confidence. It hinges on principles of **good faith, loyalty and respect for the rights of defence.**

5. The use of the internal whistleblowing system and the dedicated platform is **optional**: it is one of several whistleblowing channels, particularly for employees, who have other ways to report an issue: through hierarchical channels, the head of Human Resources, their harassment liaison officer[5] or their employee representatives.
Accordingly, an informant may not be penalised for failing to use this system. However, depending on the situation, the internal whistleblowing system may be the most appropriate channel.
What's more, it affords protection that is specific to a person's status as a whistleblower, together with stricter confidentiality.

6. The whistleblowing system does not take away a whistleblower's legal right to directly refer the matter to the **competent authorities**[6] at any time.

7. The use of the whistleblowing system is a **right** for employees. Consequently, no employee may be subject to retaliation measures or disciplinary action for having reported issues or testified in **good faith** through the whistleblowing system, even where the reported issues prove to be unfounded or inaccurate and give rise to no further action.
However, the **misuse** or use in **bad faith** of the whistleblowing system may expose the informant to disciplinary action and legal proceedings.
The use of the system in bad faith would involve using it to report issues that the informant knows to be false or to make defamatory allegations against a third party, with the intention of causing harm or in the hope of obtaining undue consideration.

8. In accordance with the law, **the employee representation bodies have been duly notified and consulted** about the Covéa internal whistleblowing system.

---

5. Covéa's harassment liaison officer: Harassment in the workplace.
6. List provided in the appendix to the French decree No. 2022-1284 of 3 October 2022 on procedures for collecting and processing whistleblowing reports and establishing a list of external authorities provided for by the law (No. 222-401) of 21 March 2022 aimed at improving protection for whistleblowers.

MAKING AN EXTERNAL REPORT

Whistleblowers are entitled to file an external report with the competent authorities, either directly or after first submitting an internal report. The competent authorities may be:

- **a judicial authority;**
- **a competent authority chosen from among those referred to in the decree ;**
- **the *Défenseur des droits* (Defender of rights), which will refer the person to the suitable authority;**
- **a competent European Union institution, body or agency.**

CHOOSING THE REPORTING CHANNEL

Informants are free to **choose the channel that seems most appropriate**, particularly when it comes to ensuring that their report will be handled effectively, impartially and in secrecy:

- **Internal reporting** is where an informant submits their report to the company to which the reported issue relates.
- External reporting is where an informant files a report with a competent authority (judicial authority for an offence, administrative authority, etc.).

Informants who are unsure which authority to contact may call on the ***Défenseur des droits***, who will refer them to the competent authority

IMPORTANT

Informants may **publicly disclose** *their report, but only in certain very specific cases governed by law. As such cases are subject to very restrictive conditions, informants are advised to raise the matter with the* ***Défenseur des droits*** *before going public.*

SCOPE OF APPLICATION

1. Only issues that are reprehensible or contrary to the public interest may be reported:

- **a crime or offence;**
- **a threat or harm to the public interest;**

- a violation or attempted concealment of a violation of national, European or international laws and regulations;
- breaches or situations that are contrary to Covéa's anti-bribery code of conduct[7];
- risks of serious harm being caused, associated with the Covéa Group's activities, in relation to human rights, fundamental freedoms, human health and safety and the environment[8].

EXCEPTIONS

Information that is covered by the following secrecy laws does not fall within the scope of the whistleblowing system, regardless of the form or the medium used:
- secrecy necessitated by matters of national defence;
- patient confidentiality relating to medical records;
- the confidentiality of investigations or judicial inquiries;
- solicitor-client privilege.

The violation of these secrecy laws is a criminal offence.

A whistleblower may only report issues in connection with the company's activities that are of an **unlawful nature** or are **detrimental to the public interest.**

Accordingly, the following cannot be used as a basis for a report:
- a simple **internal malfunction** within the company;
- **dissatisfaction** with the relationship with the Covéa Group, including employee dissatisfaction with the assessment of their performance or with their career development, except where there has been a breach of the regulations;
- an **offence committed by a third party** who was not acting on Covéa's behalf;
- customary **commercial complaints** must be sent to the competent Complaints department;
- **alerts escalated** in relation to unusual customer transactions or situations as part of anti-money laundering and counter-terrorist financing **(AML-CTF)** measures must be reported to the TRACFIN correspondent/reporting officer.

7. As part of the system for preventing and detecting acts of corruption.
8. Examples of serious breaches that may be reported under the law that requires a duty of care:
- violation of equality and privacy rights, the right to strike, or the freedom of assembly or of association,
- risk to public health, non-compliance with legal working conditions.

2. This whistleblowing system is open in particular to:
- Covéa employees, regardless of their status[9];
- external or occasional staff[10];
- former employees and job applicants;
- holders of voting rights at General Meetings (members);
- members of the Covéa Group's governance bodies;
- co-contractors of the Covéa Group and their subcontractors;
- external stakeholders with respect to duty of care failures, in connection with the Covéa Group's activities and those of its subcontractors and suppliers.

3. The Covéa internal whistleblowing system centralises the receipt of reports from Group companies that do not have their own whistleblowing system.
All reports that are received are handled efficiently and impartially in an appropriate manner according to the entity in question.

CONTACTS

1. Covéa employees can raise the issue with their usual contacts:
- their **manager,**
- the **head of Human Resources.**

2. Before using the internal whistleblowing system, they may also seek advice from the **Covéa Compliance Department** (Business Ethics division) by emailing: ethique@covea.fr.

In this case, the employee will forego whistleblower protection.

9. Employees on permanent contracts, fixed-term contracts, work-study contracts and internships.
10. Temporary workers, service providers.

WHISTLEBLOWER PROTECTION

CONDITIONS TO QUALIFY FOR LEGAL PROTECTION

To qualify for whistleblower protection, a person must satisfy all of the following conditions:

1. They must be a **natural person**: legal entities cannot be considered as whistleblowers.
2. They must derive no **direct financial gain** from the submission of the report (e.g. remuneration, bonus or raise).
3. They must be acting in **good faith**: there must be reasonable grounds to believe that the reported issues truly occurred.
4. The **issues they are reporting must fall within the scope of the whistleblowing system** (unlawful actions or situations or ones that are harmful to the public interest).
5. If the reported information was obtained outside a work-related sphere, the informant must have **personal knowledge** of it.

Conversely, where the information has been obtained within a work-related context, the informant is not required to have personal knowledge of the reported issues in order to qualify for whistleblower status.

PROTECTION PROVIDED FOR BY LAW

If the informant satisfies all the conditions to qualify as a whistleblower, they will benefit from the following protective measures:

1. The protective status bestowed on whistleblowers is **public policy**, which means that it cannot be waived by any means whatsoever.

2. **The identity of the whistleblower** must be kept secret by the persons receiving and handling reports.
Any failure to comply with this obligation may be punishable by two years' imprisonment and a €30,000 fine.

EXCEPTIONS

Information relating to the whistleblower's identity may be communicated to the judicial authorities where the company has an obligation to refer the reported issues to them. The whistleblower will be notified of this, except where such notification might compromise the legal proceedings.

3. Where the whistleblower is an employee, they cannot be punished by their employer[11] or be subjected to any retaliation measures whatsoever as a result of the submission of their report.
The French labour code (*Code du travail*) lists 15 measures that employers are prohibited from taking against whistleblowers (e.g. disciplinary measures, transfer, negative performance review, etc.).

4. Where negative measures have been taken against them, whistleblowers may refer the matter to the industrial tribunal for summary proceedings. They may also obtain compensation for any prejudice caused to them (e.g. loss of remuneration after submitting a whistleblowing report).
The employer must be able to prove that the measures taken against the employee are not connected in any way with the whistleblowing report.

5. Furthermore, the law provides for the following:
- **no civil liability can be borne by the whistleblower if their report appears to have been necessary to safeguard the interests in question and complies with the rules laid down by law.**
- **no criminal liability can be borne by the whistleblower where they have committed the offence of disclosing confidential information or a secret of which they became aware in a lawful manner, for example, in the course of their duties.**

However, the disclosure of such information must have been necessary and proportionate to the safeguarding of the interests in question.

11. Pursuant to Article L1132-3-3 of the French labour code.

6. Whistleblowers may be eligible for:
- **financial support** decided by the court hearing the case (court fees or provisional allowances where their financial circumstances have deteriorated) where legal proceedings have been undertaken;
- **measures to facilitate their reinstatement in the workplace:**
  - The industrial tribunal referral procedure allows the judge to quickly hand down a decision on a whistleblower's dismissal.
  - The judge may order the employer to contribute to the whistleblower's personal training account.
- **psychological and financial support measures** through the competent external authority.

7. Those responsible for retaliation measures or for filing a **"SLAPP" suit (strategic lawsuit against public participation)**[12] against a whistleblower face prosecution:
- preventing a person from submitting a whistleblowing report is an offence that is punishable by one year in prison and a €15,000 fine.
- wrongful recourse against a whistleblower is punishable by a civil fine of up to €60,000.

8. The protective measures are extended to the whistleblower's connections:
- "facilitators", i.e. natural persons who may risk retaliation (e.g. a co-worker) or non-profit private legal entities (association, trade union, non-governmental organisation) that support the whistleblower.
- natural persons who are connected to the whistleblower (e.g. a co-worker, friend or relative or subcontractor of the employer) or a legal entity that is connected to the whistleblower (e.g. a company that is controlled by them or that employs them).

12. For example, a defamation lawsuit in a bid to intimidate the whistleblower.

THE COVÉA INTERNAL WHISTLEBLOWING SYSTEM

1. The Covéa internal whistleblowing system is based on:

- **This procedure** which explains:
  - the conditions under which a person qualifies for whistleblower status,
  - the process for managing whistleblowing reports.
- A **secure platform** for receiving and handling reports in a secure and confidential environment.
- An **organisation** with **identified stakeholders,** detailed in the table below. The number of stakeholders is kept to a minimum. They are chosen because of the specific expertise they hold in order to process reports.

STAKEHOLDER	ROLE
WHISTLEBLOWING OFFICER	This is the Covéa Group's Chief Compliance Officer, who has been appointed by Covéa's Chief Executive Officer to oversee the receipt and handling of reports. The Whistleblowing Officer ensures that the entire internal whistleblowing system runs smoothly and chairs the Covéa Ethics Committee.
COMPLIANCE DEPARTMENT'S BUSINESS ETHICS DIVISION	Employees at the Compliance Department's Business Ethics division are tasked with collecting and processing the reports that are received. They participate in the Ethics Committee and may conduct investigations.

⟶ Table continues on next page

STAKEHOLDER	ROLE
ETHICS COMMITTEE	This committee provides support to the Whistleblowing Officer when it comes to: - analysing reports received; - conducting investigations; - the decision-making process regarding further action to be taken. It is made up of a small number of permanent members: the Head of Compliance, the Head of Internal Audit and the Head of Permanent Internal Control. Depending on the purpose and context of the report, the heads of other departments may also attend Ethics Committee meetings (namely the Head of Human Resources and the Head of Legal). This committee ensures that all the relevant departments work together to make decisions.
INVESTIGATION UNIT	The investigation unit has a small number of members, all employees, appointed by the members of the Ethics Committee. Employees with expertise in the area to which the report relates are tasked with conducting investigations to establish the veracity of the reported issues.
GOVERNING BODY	The Whistleblowing Officer keeps the governing body abreast of internal investigations relating to the most sensitive cases (particularly where a criminal offence may have been committed), except those in which the governing body is itself implicated. The information is imparted in such a way as to keep the informant's identity a secret.

2. All of these persons are bound by a specific non-disclosure provision that specifies the criminal punishment in the event that they disclose a whistleblower's identity.

3. Depending on the circumstances of the case, the Ethics Committee may decide to have the investigations carried out:
- internally by the competent members of the investigation unit,
- or externally by any authorised third party, due to their competence and/or their impartiality or due to the complexity or sensitivity of the investigation.

These third parties may be lawyers, experts or auditors, provided that they are legally or contractually bound to adhere to strict non-disclosure rules.

PREVENTING AND MANAGING CONFLICTS OF INTEREST IN THE HANDLING OF REPORTS

1. The members of the Ethics Committee are provided with the means to carry out their duties impartially and independently.
They have familiarised themselves with the main regulatory provisions governing the receipt and handling of whistleblowing reports.
They cannot be relieved of their duties or penalised in any way by their employer for performing the tasks entrusted to them in connection with this whistleblowing system.

2. The members of the Ethics Committee and all the persons involved in the receipt and handling of whistleblowing reports have undertaken not to get involved in any case that would put them in a conflict of interest.
They are therefore **required to declare** any potential, apparent or proven **conflict of interest** arising from links they may have with any person involved in a given whistleblowing report (informant, witness, victim, accused person) or from their responsibility in the process implicated by the report.
This obligation consists of reporting the conflict of interest in writing to the Whistleblowing Officer **before participating in the handling of the report or, failing that, as soon as the conflict of interest comes to light during the course of the investigation.**

3. The reported conflict of interest is then analysed by the Compliance Department's Business Ethics division and presented to the Ethics Committee along with any proposed **remedial action**. Where the conflict of interest is confirmed, the Ethics Committee will be required to approve the **remedial action** in order to resolve the conflict of interest. This may involve the person having to recuse themselves and being replaced by a substitute or the investigations being entrusted to an outside party. This measure will be formalised in writing by the Whistleblowing Officer, who will notify the person.

4. Where the Whistleblowing Officer finds themselves in a conflict of interest, the Ethics Committee will decide to entrust the investigations to an outside party, without involving the Whistleblowing Officer in this decision. The decision will be formalised in writing and notified to the Ethics Committee.

RECEIVING REPORTS

CIRCULATING INFORMATION ON THE INTERNAL WHISTLEBLOWING SYSTEM

1. To be effective, the Covéa whistleblowing system must be circulated to all employees and external stakeholders.

2. All Covéa employees are informed about the system and this procedure through internal communication and an intranet presentation of the system (in the "Compliance" section).

3. Third parties are informed about the system through publications on the corporate website www.covea.com and on the websites of the Group's brands.

4. This procedure is supplemented by a practical guide for whistleblowers.

ACCESSING THE WHISTLEBLOWING PLATFORM

1. Keeping whistleblowing reports confidential and protecting informants are fundamentally important to the Covéa Group.
That is why reports are received and handled via a secure platform with an encrypted messaging feature that is separate from the company's information systems and does not allow IP addresses to be traced.
The data is hosted on an outside server based in France.
Only authorised persons may access reports.

2. This outside platform is:
- available at all times,
- available in French and English,
- accessible from any device connected to the Internet (computer, tablet, smartphone).

3. The whistleblowing platform is easily accessible.

By employees:

- via the Covéa intranet applications (search for "Whistleblowing system" in the Apps section).

By third parties:

- via the Covéa corporate website: www.covea.com (search for "Whistleblowing system"),
- or via the following link: https://covea.whispli.com/signalement.

SUBMITTING A WHISTLEBLOWING REPORT

1. Before submitting a report using an online form, the informant will be invited to set up an account (or "inbox"). Once they have done that, they will be able to submit their report and, later on, to chat with a case manager and follow-up on the status of their report.
The Covéa Group will never have access to the credentials (identifier and email address) provided by the informant when they set up an inbox.
This means that the informant will never need to disclose their identity.
The informant can also choose to log in as a "Guest" without an inbox.

2. Before submitting a report, the informant must familiarise themselves with this procedure in order to **ensure that the situations they wish to report fall within the scope of the Covéa internal whistleblowing system.**
Where they do not fall within the scope of the system, the informant is invited to use the other existing channels or to contact the Compliance Department (ethique@covea.fr) to find out how to proceed.

3. The informant will then be able to complete the online form, in which they will be asked to describe the purpose of their report.
They will be asked to provide the most factual, precise and exhaustive information possible, which must be **directly related to the purpose of the report:**
- the issue;
- the persons involved;
- the place and date or period relating to the reported issue.

The information provided must relate to **objective facts that are materially verifiable and relevant** with regard to the alleged breaches and directly related to the purpose of the report.
This information must be detailed enough to enable an assessment of the nature, extent and urgency of the reported problem, and must be **supported by evidence**, preferably in writing.
The wording of the allegations must reflect the presumed nature of the reported issues and not infringe on the privacy of the persons referred to in the report.

4. The informant will then be able to choose whether they wish to disclose their **identity** or not. If they choose not to disclose their identity, they will be advised that:

- extra care will be taken to examine the report in order to avoid a risk of a malicious report being submitted;
- the investigations may be more time-consuming;
- they will not be able to benefit from whistleblower protection, as their identity is not known.

An informant is free to waive their anonymity at any time during the report handling process.

Where the report has been made anonymously and the informant has not provided an email address to receive notifications, they will need to **regularly log into the platform** to see if they have received any messages and respond to requests for additional information.

5. Once they have completed the online form, the informant will be invited to review a copy of the report before **validating** it.
Any mandatory fields that have not been completed will be highlighted.

6. The informant can create a draft report and send it later and may attach files to substantiate their report.

ACKNOWLEDGEMENT OF RECEIPT

Once the form has been validated and sent, the informant will immediately receive an acknowledgement of receipt in their safe inbox.

NOTIFICATIONS

Informants can choose to be notified of the receipt of a new message in their safe inbox:

- by e-mail at the e-mail address they provided when they set up their account,
- or through push notifications via the Whispli mobile app (if they have downloaded it).

CONFIDENTIALITY ASSURANCES

The Covéa internal whistleblowing system guarantees that the identity of informants who have reported an issue in good faith will be kept strictly confidential, regardless of whether or not they have whistleblower status (see conditions above), at every stage of the handling of the report.

Accordingly:

1. **End-to-end encryption**[13] will be used for the content of all reports made via the online platform.

2. All messages will be sent and received via a **safe inbox** hosted on the whistleblowing platform and will remain confidential.

3. Only a small number of people will be authorised to receive and handle reports and they will be bound by **specific non-disclosure rules.**

4. Where applicable, the experts assigned to conduct the investigations will be contractually bound to keep the data relating to the report private and to delete it once they have completed their assignment.

5. Information that might reveal the whistleblower's identity will never be disclosed to the persons referred to in the report: alleged perpetrator(s) of the reported issues, victim(s) or witness(es).

6. Where a report is made **anonymously**, the platform will ensure that any further communication with the informant will also be conducted anonymously. No process[14] will be triggered that might reveal the informant's identity.

13. AES-256 encryption.
14. Such as: collection of the IP address, use of cookies.

HANDLING REPORTS

1. The report handling phase begins once the report has been received on the platform. It ends once a decision has been made as to any follow-up action and this decision has been notified to the informant and the person(s) referred to in the report.

2. At each stage of the process, messages will be sent to the informant's safe inbox to inform them of the:

- receipt of the report via an **acknowledgement of receipt** issued immediately after the report has been submitted on the platform;
- **inadmissibility** of the report, where this is the case;
- **report's handling status** within 3 months of its receipt;
- **completion of investigations** and the closure of the report, together with the main steps taken to remedy the situation, if any.

ANALYSING REPORT ADMISSIBILITY

1. The admissibility of reports is analysed to determine whether they fall within the scope of the internal whistleblowing system and comply with the conditions laid down by law.

2. This analysis, which may require some preliminary investigations, is carried out by the Business Ethics division.
During this phase, the informant may receive messages in their safe inbox asking them to provide additional information or to clarify some aspects of their report. If this is the case, the informant will receive a notification (by email or via the app) inviting them to log into the platform.
If they have not activated the notification feature, they will need to log in regularly.

3. The findings of the admissibility analysis will be submitted to the Ethics Committee for validation.

4. The Ethics Committee will then decide whether the report is admissible and determine what subsequent action should be taken, if any:
- Where the report is deemed inadmissible, the informant will receive a message that the report has been closed with the reasons for this decision.
- Where the report is deemed admissible, the committee will appoint people with expertise in the area covered by the report to conduct an investigation.

5. Where a **report has been submitted anonymously**, the Whistleblowing Officer will ensure that special precautions are taken in the handling of the report, particularly during the prior admissibility review, by ensuring that the reported issues are sufficiently credible, serious and detailed. Anonymous reports that are deemed admissible will be handled in the same way as all other admissible reports, provided that the informant responds to any requests for additional information during the course of the investigations within a reasonable time frame.
Where the report has been made anonymously and the informant has not provided an email address to receive notifications, they will need to regularly log into the platform to see if they have received any messages and respond to requests for additional information.
Failing this, and if the report does not contain sufficiently detailed information to conduct an investigation in order to determine the accuracy of the reported issues, it will be closed without further action.

INVESTIGATIONS

1. Investigations into admissible reports will be carried out by authorised persons appointed by the Ethics Committee. Only persons specifically authorised to process reports may have access to them. The Whistleblowing Officer and their team will conduct or coordinate the investigations.

2. The purpose of these investigations will be to verify the materiality and accuracy of the reported issues.
The whistleblowing platform will keep a record of all the procedures carried out in the course of the investigation (legal and technical analysis of the reported issues, application of precautionary measures, gathering of evidence, communications and/or interviews with stakeholders, interviews with witnesses or persons who may provide relevant information relating to the reported issues, completion of expert appraisals, etc.).

3. All necessary **precautionary measures** will be taken to safeguard evidence substantiating the reported issues.

4. Once these measures have been taken, the Whistleblowing Officer will **inform the person implicated** in the report in **writing** that their personal data will be processed in connection with the whistleblowing system.

5. The investigation process may require questions to be put to the informant via the secure platform in order to obtain additional information or details. The informant will be expected to respond within a reasonable time frame to facilitate the proper conduct of the investigation.

6. The informant may, at any time and on their own initiative, use the secure platform to send additional supporting information or documents which may have come to their attention after they submitted their initial report.

7. At the end of the investigation period, the person(s) assigned to conduct the investigation will prepare a written report for the Ethics Committee on the verifications they have carried out, their findings and their conclusions, together with proposed measures.

8. In any event, the informant will receive **a status update within 3 months** of the date of the acknowledgement of receipt of their report. This update will relate to:
- the investigative measures taken to establish the accuracy of the reported issues,
- as well as any remedial measures taken.

DECISIONS TAKEN FOLLOWING INVESTIGATIONS

1. The Ethics Committee will decide what action should be taken on the report:
- it may be closed without any further action if the reported issues have not been proven, the investigation has not established the veracity of the alleged issues or if insufficient evidence has been gathered.
- it may be followed up with further action if the reported issues have been proven.
- This follow-up action may include:
  - internal remedial measures, such as: measures to enhance a process, raise awareness or train the relevant employees, issuance of a reminder of the rules that apply, communication actions;
  - a termination of the contractual relationship with a third party (if they are implicated);
  - disciplinary measures;
  - legal action.

2. The Ethics Committee will hand the case over to the competent department so that it can take the necessary action.

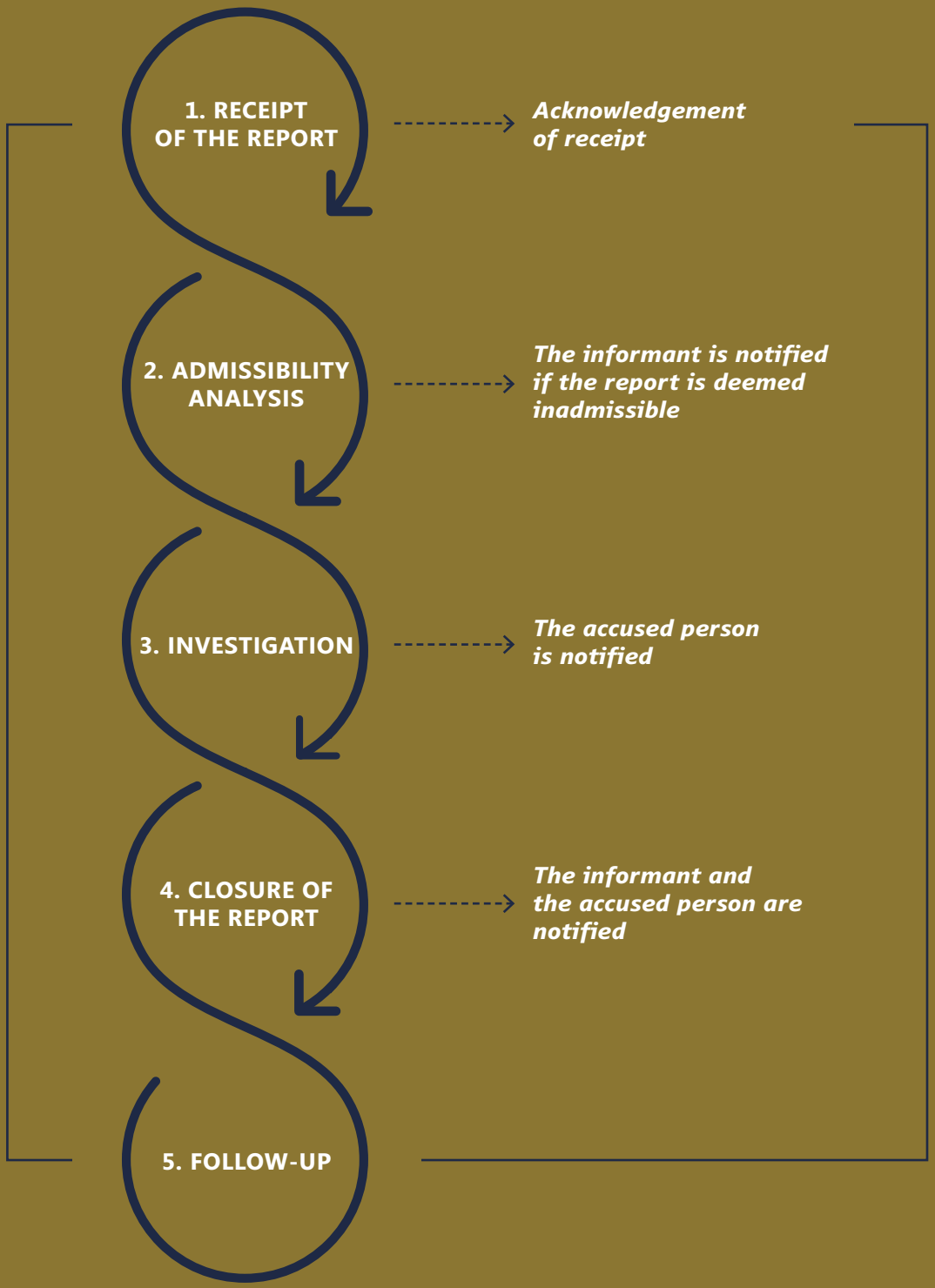
CLOSING A REPORT

1. Whatever the outcome of a report, the informant will be systematically notified in writing of the closure of the report and of the decision that has been taken following the investigation.

2. The person(s) referred to in the report will be notified by any appropriate means of the follow-up that will be given to the report, either by the Whistleblowing Officer or by a member of the Ethics Committee.
If, on completion of the investigation, an employee is found to be implicated, the Human Resources Department will notify them according to the procedure in place.

3. Personal data will be retained and then anonymised or deleted in accordance with the personal data protection policy described below.

SUMMARY


1. RECEIPT OF THE REPORT
Acknowledgement of receipt
2. ADMISSIBILITY ANALYSIS
The informant is notified if the report is deemed inadmissible
3. INVESTIGATION
The accused person is notified
4. CLOSURE OF THE REPORT
The informant and the accused person are notified
5. FOLLOW-UP

REPORTING ON THE INTERNAL WHISTLEBLOWING SYSTEM

The Whistleblowing Officer draws up an annual, fully anonymised, report covering all the whistleblowing reports received and handled in the past year.

This report contains a quantitative and qualitative analysis of the data (namely, the type of themes covered by the reports, the admissibility rate and the type of follow-up action).

It is submitted to the Covéa Ethics Committee and to the Covéa management body each year.

PERSONAL DATA PROTECTION POLICY

1. WHO PROCESSES THE DATA?

Personal data is processed by the employer, if the person is an employee of the Covéa Group, and by the group to which they belong (the Covéa Group), which are the data controllers. The employer's contact details are shown on the employment contract or payslips. The Covéa Group is represented by Covéa, a mutual insurance group company governed by the French insurance code, registered on the Paris trade and companies register under No. 450 527 916, with its registered office at 86-90 Rue Saint Lazare 75009 Paris.

Additional information on the Covéa Group is available:
- for employees: in the "About our Group" section, accessible from the "My knowledge base" section of the intranet site,
- for everyone: on the Group's website: www.covea.com.

2. WHAT TYPES OF DATA ARE PROCESSED?

Data is processed where an individual reports information relating to the following:
- a crime, offence, threat or harm to the public interest or a breach of regulations;
- breaches or situations that are contrary to Covéa's anti-bribery code of conduct;
- risks of serious harm being caused, associated with the Covéa Group's activities, in relation to human rights, fundamental freedoms, human health and safety and the environment.

The following types of data are processed:
- customary identification data (identity, position, department to which a person is assigned and contact details), regardless of whether the person is the informant (assuming they have elected to disclose their identity, given that they may also submit an anonymous report) or whether they are referred to in the report;
- the elements associated with the report, where they can be connected to the data (reported issues and elements to verify them, report on the verifications carried out, any follow-up action).

3. WHY IS THIS DATA PROCESSED?

The data is used to process reports of crimes, offences, threats or harm to the public interest, breaches of regulations, breaches of Covéa's anti-bribery code of conduct or violations of human rights and fundamental freedoms and risks of serious harm to human health and safety and the environment, and more specifically to:

- receive and handle reports;
- carry out the necessary checks, investigations and analyses;
- determine any follow-up action;
- ensure the protection of the persons involved and, in particular, to ensure that the informant's identity and any subsequent communication with them is kept private, as well as the reported issues and the persons referred to in the report;
- exercise or defend legal rights.

This purpose has as its legal basis the regulatory obligations of the employer and the Covéa Group.

In addition, information relating to personal data privacy will be specifically provided to the person(s) referred to in the report within a reasonable time frame of no more than one month following receipt of the report, using any appropriate means (letter, email). However, the communication of this information may be postponed if there is a chance it might seriously compromise the achievement of the data processing objectives. This information will only be communicated once precautionary measures have been taken to prevent the destruction of evidence relating to the reported issues and the report has been deemed admissible.

4. TO WHOM WILL THE DATA BE SENT?

The data may be communicated to the following persons, within the limits of their assignments and authorisations:

- the persons within the Covéa Group who are tasked with receiving and managing reports,
- the service provider(s) to which the employer or the Covéa Group may subcontract the management of certain tasks,
- experts assigned for the purposes of the investigation,
- the judicial authority, if needed.

5. HOW LONG WILL THE DATA BE RETAINED?

The data retention period will depend on the status of the report:

- Reports are kept until a final decision has been made on the next steps to be taken.

- Once a final decision has been made on follow-up action, there are three possible scenarios:
  - Where the report has been deemed inadmissible because it does not fall within the scope of the internal whistleblowing system, the data will be retained for three months from the date on which the informant has been notified of the report's inadmissibility in order to address any questions the informant may have regarding this decision.
  - Where the report has been deemed admissible and has either been closed without further action or has had non-disciplinary or non-judicial consequences, the data will be retained for one year from the date of the decision, in order to:
    - protect the various people involved (informant, facilitator, person mentioned in or referred to in the report) from the risk of retaliation measures.
    - allow for any additional investigations.
    - provide evidence on the manner in which the report has been handled in the event of a dispute or subsequent controls on the compliance of the report handling process (audit, authority).

- Where the report has been deemed admissible and has ultimately led to disciplinary or judicial action being taken against a person referred to in the report or against a person having submitted a spurious report, the data will be retained until the end of the procedure or until the end of the limitation period for appeals against the decision.

Once these retention periods have ended, the data will be anonymised or deleted.

6. WHERE IS THE DATA PROCESSED?

The data will be processed in France. Exceptionally, data may be processed outside the European Union where this is deemed suitable or where contractual terms have been set to provide for this. These terms can be obtained from the Data Protection Officer.

7. WHAT ARE THE RIGHTS OF THE PERSON WHOSE DATA IS BEING PROCESSED?

The data subject has a right to access their data, to limit its processing and to have it rectified or erased.

Under the **right of access**, the data subject may request:
- confirmation that the data relating to them is (or is not) processed;
- a copy of all the personal data relating to them that is in the possession of the data controller.

The right of access does not give a person referred to in a report the right to acquire knowledge of the informant's identity or of any data relating to third parties.

The **right to request rectification** entitles the data subject to have information relating to them rectified when it is obsolete or incorrect. It also gives them the right to add information relating to them when their information is incomplete.

The **right to request erasure** entitles the data subject to have their personal data erased subject to the statutory retention periods. This right may apply, in particular, where the data is no longer required for processing purposes.

The **right to request limitation** entitles the data subject to request that the processing of their data be limited in the following cases:
- where their data is used unlawfully;
- where the data subject disputes the accuracy of the data;
- where the data subject needs to have the data to establish, exercise or defend their rights.

The data subject may exercise their rights by writing to the following addresses:

- for employees of the Covéa Group:
  - by post: Covéa - Droits d'accès RH – 86-90 rue Saint Lazare 75009 Paris,
  - by email : protectiondesdonneesrh@covea.fr ;

- for all other persons:
  - by post: Covéa - Délégué à la Protection des Données – 86-90 rue Saint Lazare, 75009 Paris,
  - by email: delegueala protectiondesdonnees@covea.fr.

The data subject may also give general instructions to a trusted third party or specific instructions to the data controller regarding the retention, erasure and communication of their personal data after their death. These instructions may be modified or revoked at any time.

In the event of disagreement over the processing of their personal data, the data subject may refer the matter to the Commission Nationale de l'Informatique et Libertés (CNIL - French data protection commission).

8. HOW CAN I CONTACT THE DATA PROTECTION OFFICER?

Any queries can be sent to the Data Protection Officer:

- for employees of the Covéa Group:
  - by post: Covéa - Droits d'accès RH – 86-90 rue Saint Lazare 75009 Paris,
  - by email: protectiondesdonneesrh@covea.fr ;

- for all other persons:
  - by post: Covéa - Délégué à la Protection des Données – 86-90 rue Saint Lazare, 75009 Paris
  - by email: delegueealaprotectiondesdonnees@covea.fr.

GLOSSARY

INFORMANT

Person who submits a report. Informants who satisfy all legal provisions will be given whistleblower status.

EXTERNAL AUTHORITIES

These are:
- the competent judicial authority where the reported issues constitute a crime or an offence,
- the competent authorities in the field to which the report relates.

EXAMPLES

AUTHORITY	REMIT
ACPR French prudential supervision and resolution authority	financial services, products and markets, the prevention of money laundering and terrorist financing
CNIL French data protection agency	privacy and personal data protection, network and information system security
DGCCRF Directorate general for competition policy, consumer affairs and fraud control	consumer protection, anti-competitive practices (internal market)
DGT Directorate general for labour	individual and collective labour relations, working conditions

DÉFENSEUR DES DROITS

The Défenseur des droits (Defender of rights) is an independent French administrative authority that works to uphold the rights and freedoms of citizens. It provides support for whistleblowers who request it (information, advice, referrals, support).
It also handles whistleblowing reports brought to its attention that fall within its remit (discrimination, children's rights).

PUBLIC DISCLOSURE

Where a whistleblower makes their report public, particularly through the media.
In order to retain whistleblower status, they may only publicly disclose a report under certain conditions provided for by law.

FACILITATOR

Person who helps the whistleblower:
• a natural person: co-worker, friend or relative,
• a non-profit private legal entity: association, trade union, NGO.
A facilitator who acts within the letter of the law when they provide help to a whistleblower may qualify for the same protection as the whistleblower.

WHISTLEBLOWER

Person who has submitted a whistleblowing report and meets all the legal requirements to qualify for the protective status afforded to whistleblowers.

RETALIATION MEASURES

Adverse measures taken against a whistleblower.
The French labour code lists 15 such measures and prohibits them where they relate to whistleblowing.

ACCUSED PERSON

Person identified in the report as the person having committed the reported issues.

PERSON REFERRED TO IN THE REPORT

Any natural person mentioned in the report:
- alleged perpetrator of the reported issues,
- victim,
- witness.

WHISTLEBLOWING OFFICER

Person appointed and authorised to receive and handle reports falling within the scope of this system.

INTERNAL REPORTING

Report made to the entity to which the reported issues relate. In order to qualify for whistleblower status, the informant must follow the internal procedure in place within the professional structure they are dealing with.

EXTERNAL REPORTING

Report made to a competent external authority.
Informants may now file a direct report with the authorities without having to go through internal channels beforehand.

AUTHORISED THIRD PARTY

Any third party appointed by the Whistleblowing Officer and/or the Ethics Committee to examine all or some of the reported issues.

The digital version of this document is compliant with the PDF/UA (ISO 14289-1), WCAG 2.1 level AA and RGAA 4.1 accessibility standards with the exception of the colour criteria. Its design enables people with motor disabilities to browse through this PDF using keyboard commands. Accessible for people with visual impairments, it has been tagged in full, so that it can be transcribed vocally by screen readers using any computer support.

Accessible PDF powered by DocAxess

MUTUAL GROUP INSURANCE COMPANY
governed by the French Insurance Code
RCS Paris 450 527 916
86-90, rue Saint-Lazare - 75009 Paris

Find us on social media @groupecovea and at covea.com