



# Whistleblowing policy

The French version is the reference version in French-speaking countries.

The English version is the reference document in other countries.



©SERIS Group – August 2025

All rights reserved.

## Preamble

At SERIS, we want to detect possible fraudulent or unethical behaviour at an early stage to protect effectively our company, our employees, our customers and our partners.

That is why we encourage our employees and all our stakeholders to report any regulatory or ethical concerns to us, so that we can take the necessary corrective action.

Our internal whistleblowing policy is based on the principles of good faith, loyalty and respect for defence rights.

Our internal whistleblowing system enables employees and stakeholders to make a report within a secure, effective framework that offers them every guarantee of confidentiality, in accordance with the applicable legislative provisions, and in particular in France, the "Sapin II" and "Duty of Vigilance" laws.

These guarantees allow them to reveal serenely any potential violation of our ethical rules, as well as any threat or harm to the general interest.

SERIS protects whistleblowers who act in good faith against any form of retaliation.

The content of this Group policy may sometimes differ from applicable local law.

In this case, the rules that are most protective of whistleblower will apply, whether they derive from local legislation or from this policy.

The Group's Chief Legal and Compliance Officer is SERIS's permanent point of contact for managing whistleblowing and conducting ethical investigations.

In this document, "SERIS" refers to GenTem SAS and all its direct or indirect subsidiaries.

### **Guy TEMPEREAU**

President of the Governance and Animation Board of GenTem

### **Bruno CATHELINAIS, Antoine MASSIET DU BIEST, Audrey PROU, Céline TEMPEREAU- SAUVAGE,**

### **Sébastien TEMPEREAU**

Members of the Governance and Animation Board of GenTem

### **Benoît PEDOUSSAUT**

President of the Group Executive Committee

### **Christophe BRASSELET, Tibo DEMOOR, Patrick FERHAT, Eric FORESTIER, Sophie LECLERC, Philippe MAURETTE, Sylvia MULLER, Daniel MURCIANO**

Members of the Group Executive Committee

## Contents

<b>1. Conditions governing the admissibility of a report.....</b>	<b>5</b>
1.1 Who can make a report ?.....	5
1.2 What are the conditions for benefiting from the legal protection granted to whistleblowers ? .....	5
1.3 What can be reported? .....	6
<b>2. How to make a report.....</b>	<b>9</b>
2.1 How do I report an incident ? .....	9
2.2 Is it possible to make an anonymous report? .....	10
2.3 What information should be provided in support of a report? .....	11
<b>3. Processing a report.....</b>	<b>13</b>
3.1 Who is involved in processing reports? .....	13
3.2 How is the admissibility of a report assessed? .....	15
3.3 How is the investigation carried out following an admissible report? .....	16
3.4 What happens at the end of an internal investigation? .....	17
3.5 To sum up .....	19
.....	20
<b>4. Rights, duties and obligations of persons involved in an ethics report.....</b>	<b>21</b>
4.1 How is the confidentiality of information gathered in the context of a report protected? .....	21
4.2 Is collaboration to an internal investigation mandatory? .....	22
4.3 What information is passed on to the people involved? .....	22
4.3.1 Informing the whistleblower.....	22
4.3.2 Informing the alleged perpetrator .....	23
4.3.3 Informing witnesses .....	23
4.4 How is whistleblower protected against retaliation? .....	23
4.5 What are the sanctions in case of a breach of this whistleblowing policy? .....	24
4.6 How is whistleblowing system monitored at Group level? .....	24
4.7 Are there any other ways of reporting? .....	24





# 1

**Conditions governing the  
admissibility of a report**

## 1. Conditions governing the admissibility of a report

### 1.1 Who can make a report

The SERIS whistleblowing system is open to the following people:

- **Employees of SERIS**, currently working or having worked for SERIS, whatever the nature of their employment contract (permanent, fixed-term, part-time, etc.);
- **Occasional employees**, in particular temporary staff, trainees, apprentices, as well as any person working under the supervision and direction of SERIS contractors or subcontractors;
- **Candidates for employment with SERIS**, or future employees whose employment relationship has not yet begun;
- **Shareholders, associates or holders of voting rights** at SERIS general meetings;
- **Corporate officers of SERIS, members of a governance, management, administrative or supervisory body of a SERIS entity**, including past or present non-executive members;
- SERIS's **external partners** (suppliers, subcontractors, service providers, associations, etc.);
- SERIS **customers**.

### 1.2 What are the conditions for benefiting from the legal protection granted to whistleblowers ?

To benefit from the protection afforded to whistleblowers, it is necessary to meet all of the following conditions:

- You have to **be a natural person**: legal entities are not considered whistleblowers.
- You must **not receive any direct financial compensation as a** result of reporting (e.g. pay, bonus or increase).
- You must **act in good faith**: the whistleblower must provide information that he or she believes to be complete, fair and accurate, enabling him or her to believe reasonably that the information reported is true, even if it later transpires that it was a mistake. If, after having made a report, the whistleblower realises that he or she was mistaken, he or she must immediately inform the person to whom he or she made the report.

- You must **report facts that meet the requirements and conditions of the whistleblowing system** (i.e. facts that are illegal or detrimental to the public interest, see point **1.3** below).
- If the information reported was obtained outside the professional context, it is necessary to **have had personal knowledge of these facts**. On the other hand, if the information was obtained in the course of a professional activity, it is not necessary to have had personal knowledge of it (it may be facts that were reported to the person making the report).

The protection of the whistleblower is extended:

- Facilitators (any natural or legal person under private law, not for profit, who helps the whistleblower to make his/her report);
- Individuals in a relationship with the whistleblower (i.e. all those who might be subject to retaliation in the course of their professional activities on the part of their employer, their client or the recipient of their services) and ;
- Legal entities for which the whistleblower works or with which he/she has a professional relationship or which he/she controls.

## 1.3 What can be reported?

Making a report involves disclosing **facts that are reprehensible or contrary to the public interest**:

- **Criminal activity** (a felony or misdemeanour);
- **Violation of** a national, European or international **law or regulation**;
- **Violation** of the SERIS **anti-corruption code of conduct** or any other Group compliance or ethics policy;
- A situation that may present **a threat or harm to the general interest**;
- **Infringement or risk of infringement of human rights, fundamental freedoms, personal health or safety, or the environment**;
- **Intentional concealment of such acts**.

Information considered to be national defence classified information, or private medical information, or attorney-client privileged information, or information covered by confidentiality with regards to state investigations or judicial enquiries, may not be reported, as the violation of such legal or professional confidentiality commitments might be unlawful and subject to criminal penalties.

The report must relate to **facts connected with the activities of SERIS** (information obtained in the course of your professional activities, even if you are not or are no longer an employee or facts that have occurred or are likely to occur in the company or in its relations with third parties).

Concerns which do not fulfil these requirements (for example: internal dysfunctions, dissatisfaction linked to relations with SERIS, employee dissatisfaction with their performance evaluation or career development (unless there is a breach of the regulations), normal commercial complaints) will not be considered as reports under this policy. These concerns can be shared via the usual contacts of the stakeholder involved (SERIS management, Human Resources, Client contact, etc.).

In concrete terms, and by way of illustration, the **main incidents that may be reported under this policy include** the following:

- **Human rights and fundamental freedoms:**  
For example: sexual harassment, including sexist comments, bullying, discrimination, including racist, anti-Semitic or homophobic comments, human rights abuses in our supply chain (e.g. child labour or forced labour at our suppliers' sites), and so on.
- **Personal health, safety and security:**  
For example: non-compliance with regulations designed to protect health at work, unsafe working conditions (at SERIS or in the supply chain), epidemic situations, lack of safety equipment or procedures on a site, etc.
- **Economic and financial interests:**  
For example: conflicts of interest, private or public corruption, influence peddling, internal or external fraud, breaches of competition rules, money laundering, misappropriation of funds, disclosure of sensitive information, misuse of corporate assets, etc.
- **The environment:**  
For example: pollution of the air, soil, surface or ground water, release of toxic substances, etc.
- **The Code of Conduct and other Group charters or ethical policies:**  
For example: any allegation concerning behaviour that does not comply with SERIS's ethical commitments that could affect its stakeholders or its reputation.



# 2

## How to make a report



## 2. How to make a report

### 2.1 How do I report an incident ?

Anyone wishing to report an incident can do so:

- Either **via** SERIS's **secure online whistleblowing platform**

<https://serisethics.integrityline.app> (referred to as **SERISETHICS**)

This external platform, developed by EQS (an independent external company recognised for its compliance expertise), is easily accessible and offers **optimum guarantees of security and confidentiality**.

This is an area of exchange disconnected from SERIS's information systems; the data is hosted on a server external to the company, located in France.

Only authorised persons may access reports. These authorised persons are identified in point **2.2** below.

This external platform is:

- available 7 days a week, 24 hours a day;
- available in French, Polish, Dutch and English,
- accessible from any device connected to the internet (computer, tablet, smartphone).

Whistleblowers are invited to complete an online form. The description of the event or events reported can be sent **by text or voice message**.

For each report, the whistleblower is invited to create a secure mailbox, which will enable him/her to consult the platform at a later date to discuss with the Case Manager in charge of processing his/her report and to monitor the processing.

- Or **by post** addressed to :

SERIS Group  
Legal and Compliance Department  
6 rue du Général de Larminat  
75015 Paris France

It is preferable to send the letter by registered delivery with acknowledgement of receipt to ensure that it is sent securely and to establish the date of the report, and to mark the envelope containing the report and any documents with the words "**Personal & Confidential**".

Awareness of the SERIS whistleblowing system among employees and external stakeholders is essential to its effectiveness.

All SERIS personnel are informed of the existence of the system and this whistleblowing policy through internal communications in various formats (Intranet, posters, etc.).

Third parties are informed of the existence of the system by means of information on the corporate website [www.seris-group.com](http://www.seris-group.com) and the SERIS websites in the various countries in which it operates.

In accordance with the law, these internal report channels guarantee the strict confidentiality of the identity of the whistleblower, the persons referred to in the report and any third party mentioned in the report, as well as the confidentiality of the information gathered by all the recipients of the report.

The use of these two reporting channels is optional and the choice of channel is free.

**As an alternative, employees can of course contact directly their managers or human resources.**

In addition, local reporting channels that predate the SERISETHICS platform (dedicated email addresses, hotlines, etc.) may be maintained. The relevant country services are responsible for informing employees about whether or not these channels will remain in place.

External stakeholders can also make a report to their usual contact at SERIS.

However, it is preferable that reports likely to constitute admissible reports according to this policy be forwarded immediately to the persons authorised to receive and process such reports (see point 3.1. below).

## 2.2 Is it possible to make an anonymous report?

SERIS's secure whistleblowing platform makes it possible to report incidents anonymously.

The whistleblower creates a **password** and receives a **file number** generated automatically and randomly by the platform, which enables him/her to connect to a **secure mailbox** on the platform and to communicate with a Case Manager without his/her identity being revealed, if he/she so chooses. The confidentiality of exchanges is technically guaranteed by the absence of cookies, means of tracking the user and encrypted exchanges.

However, in the case of an anonymous report, the possibility of processing it under this system will depend in particular on the existence of sufficiently detailed factual information and the availability of the anonymous whistleblower to respond to requests for clarification from the Case Manager.

If anonymity makes it impossible to deal with a report, the whistleblower will be informed via the platform's secure mailbox.

Whistleblowers are advised to identify themselves at the time of reporting. Their identity will be treated confidentially in accordance with this whistleblowing policy and will not be communicated to the person reported or suspected without their explicit consent.

## 2.3 What information should be provided in support of a report?

**The information provided as part of a report must be factual and directly related to the incident reported.**

To ensure that reports are dealt with appropriately, the information provided must relate to **objective facts that are materially verifiable** and **relevant** to the alleged breaches.

This information must make it possible to assess the nature, extent and urgency of the incident reported, and must be **supported by evidence, in writing if possible**.

When in doubt, the allegations must be worded **in such a way as to show the presumed nature of the facts** and not to intrude on the privacy of the persons concerned.

In his/her report, the whistleblower should describe, as objectively as possible and in detail, the facts that led to the report to be understood. It is recommended that the whistleblower specify the following elements:

- When and where did each event take place?
- How he/she became aware of it (directly or indirectly) and whether this knowledge is personal;
- If he/she has already shared his/her report with other people ;
- If steps have already been taken to remedy the situation ;
- The identity and functions of the persons involved ;
- If anyone witnessed the events reported (identity, functions, events concerned, role of each person identified);
- If, to his/her knowledge, at the time the report is transmitted and while it is being processed, legal or similar proceedings (arbitration, mediation, injunction, etc.) are imminent or in progress. In this case, the report is deemed not admissible and its processing is therefore suspended or stopped. SERIS nevertheless reserves the right to examine the report and take corrective action if necessary.



# 3

## Processing a report



## 3. Processing a report

### 3.1 Who is involved in processing reports?

SERIS's internal whistleblowing system is based on an organisation made up of a limited number of people, chosen for their respective skills, required to deal with reports.

INVOLVED PERSON	ROLE
<b>COMPLIANCE OFFICER</b>	Group's Chief Legal and Compliance Officer. She is a member of the Ethics Committee. She is responsible for ensuring that the entire system operates smoothly. She has access to all reports and acts as a counsel and coordinator.
<b>CASE MANAGER</b>	These are employees appointed by the Ethics Committee, on the recommendation of the Compliance Officer. They are chosen based on their expertise within the Legal, Finance, and HR Departments and only receive reports that concern their perimeter and area of expertise. They process and monitor these reports. In particular, they analyse the admissibility of reports and conduct first-level investigations.
<b>INVESTIGATION UNIT</b>	Set up specifically to carry out each thorough internal investigation, it is made up of one to three members of the Ethics Committee appointed by the Chairman of the Ethics Committee on the recommendation of the Compliance Officer. Among the members of the Ethics Committee, only those who are part of an Investigation Unit may have access to the details of a report insofar as they are in charge of an investigation about such report. The Investigation Unit supports the Case Managers in dealing with reports that require a thorough investigation, if necessary.
<b>ETHICS COMMITTEE</b>	Chaired by the Chairman of the Group Executive Committee, it analyses the results of first-level investigations and thorough investigations that reveal misconducts, makes recommendations to the Governing bodies in charge to take actions. It also monitors general data on reports presented to it on a regular basis by the Compliance Officer.
<b>GOVERNING BODY</b>	Governing Bodies (Executive Committee and Governance and Management Board at Group Level, and Management Committees in the countries) are informed, within their area of competence, and excluding any member involved, of first-level investigations and thorough investigations that have revealed misconducts and of associated recommendations by the Ethics Committee. Governing Bodies decide what action to take in response to an alert, based on the recommendations of the Ethics Committee.

In accordance with the "four eyes" principle, **each report is received by two Case Managers** whose perimeter of competence and skills are adapted to process such report. Both Case Managers decide together which one of them, in accordance with their respective expertise, shall be responsible for processing the report, while the other Case Manager is there to provide support and prevent any errors, omissions or fraud.

Case Managers are SERIS employees authorised to receive and process reports. In carrying out their duties, they act under the aegis of the Group Legal and Compliance Department. They only receive reports that they are required to process or supervise, within their field of expertise.

It is important that the whistleblower carefully completes the online report form, in particular the fields relating to the **location of the incident** (France or Poland, for example) and the **subject matter of the report** (corruption, theft or safety at work, for example) so that the report can be sent to the Case Manager(s) with the technical skills required (HR, finance or law) to analyse it as effectively as possible.

Case Managers have the skills, authority and resources to carry out their role in a confidential, professional and impartial manner.

The network of Case Managers is made up of Directors from Legal, Finance and HR departments, at Group level and in each country. Each Case Manager may propose the appointment of two Deputy Case Managers in his/her department, with appropriate expertise and autonomy, to proceed with him/her with the management of reports.

The appointment or replacement of a Case Manager or Deputy Case Manager (each referred to hereunder as a "**Case Managers**") is the sole responsibility of the Ethics Committee. Only Case Managers appointed by the Ethics Committee are authorised to handle reports received on the **SERISETHICS** platform.

Depending on the specific needs of a case, an **Investigation Unit** is appointed by the President of the Ethics Committee, on Compliance Officer proposal, to conduct a thorough internal investigation.

The Investigation Unit may entrust all or part of the investigations to a third party, based on their skills and/or impartiality or because of the complexity or sensitivity of the investigation. Such third parties may include lawyers, experts and auditors, provided they are bound by law or by contract to a strict obligation of confidentiality.

By signing a **Letter of Commitment**, each Case Manager personally undertakes to comply with the following obligations:

- **Strict confidentiality obligation** applied to whistleblowing procedures, protecting the identity of the whistleblower (when it is not anonymous); the identity of persons mentioned or involved in the whistleblowing; and all information gathered during the processing. However, this information (with the exception of the identity of the whistleblower as such) may be subject to controlled and restricted disclosure for the purposes of the investigation.
- **Obligation of impartiality:** the Case Manager acts professionally, without prejudice, and does not represent any particular interests when carrying out his/her duties.

- **Obligation of transparency and loyalty** with regard to the persons whose data is processed: the Case Manager keeps the whistleblower and the persons mentioned or referred to in the report informed, in accordance with the terms and conditions of this policy.
- **Obligation to declare and withdraw in the event of a conflict of interest:** the Case Manager must inform the Compliance Officer of any potential, apparent or proven conflict of interest due to his/her links with a party involved in the report (whistleblower, witness, victim, alleged perpetrator) or his/her responsibilities in the process affected by the report; if the conflict of interest is proven, the report will be processed by another Case Manager.

The Compliance Officer and the Ethics Committee ensure that these principles are strictly complied with by the Case Managers.

Any person who is not an authorised person and who receives information that could constitute a report must inform the Compliance Officer or ask the person they are dealing with to make a report in accordance with the procedure set out in point **2.1.** above.

**Please note:** If the report concerns a member of the Ethics Committee, it is possible to specify this in the form to be completed on the platform. In this case, no member of the Ethics Committee is aware of the report. It is automatically forwarded to the Independent Directors of GenTem's Governance and Management Board, who are then responsible for processing it with a level of guarantees equivalent (in terms of deadlines, confidentiality, etc.) to that set out in this policy. The names of the Independent Administrators can be found on the corporate website [www.seris-group.com](http://www.seris-group.com). They will process the report, and will have the right to call on any person within or outside the Group to carry out any investigation (in complete confidentiality with regard to the Ethics Committee) and will inform directly the Governance and Management Board of the follow-up to the report and of their recommendations, so that a decision can be taken.

### 3.2 How is the admissibility of a report assessed?

**Each report is subject to an admissibility analysis.** The admissibility check consists of verifying whether the report meets the definition of a report under this policy and whether there are sufficiently detailed factual elements to allow it to be processed.

This analysis is carried out by the Case Manager in charge of the report and, if necessary, with the support of the Compliance Officer in the event of difficulty.

During the admissibility analysis phase, it may be necessary to obtain further information or clarification from the whistleblower. In this case, the whistleblower will receive an e-mail inviting him to log in to the platform (or will be contacted by any means he/she has chosen in the case of a report by post).

In the event of an anonymous report, the whistleblower cannot be contacted to provide the information required for the admissibility analysis. He/she must log in regularly to the platform's secure mailbox (using his/her file number and password) to check his/her messages and respond to requests for further information.

The Case Managers ensure that special precautions are taken when dealing with anonymous reports, particularly at the time of the preliminary examination of admissibility, by ensuring that the facts reported are sufficiently credible, serious and detailed.

Failing this, and if the report does not contain sufficiently detailed information to enable investigations to be carried out to establish the accuracy of the facts, the case will be closed without further action.

Anonymous reports considered admissible are treated in the same way as other reports, provided the whistleblower responds to requests for further information during investigations within a reasonable timeframe.

- **If the report is not admissible**, a message will be sent to inform the whistleblower that it has been **closed** and the reasons for this.
- **If the report is admissible**, it is subject to a first-level investigation by the Case Manager
  - If the **first-level investigation reveals that the facts reported are not established**, a message will be sent to inform the whistleblower that it has been **closed** and the reasons for this
  - If the **first-level investigation reveals that the facts reported are established**, the results of the investigation are **passed on to the Compliance Officer and the President of the Ethics Committee**, for actions to be taken (Cf. 3.4)
  - If the **first-level investigation is insufficient to establish the truth of the allegations**, then the report is forwarded to the Compliance Officer and the President of Ethics Committee (if necessary in an anonymised version to comply with the confidentiality undertakings described in this policy). Based on the information transmitted, **the President of the Ethics Committee decides on the action to be taken and, if necessary, appoints the members of the Investigation Team who will be responsible for carrying out a thorough investigations** depending on the area to which the report relates, in accordance with the Group's internal investigation procedure.

### 3.3 How is the thorough investigation carried out following an admissible report?

Depending on the results of first-level investigations carried out by Case Managers, **the President of the Ethics Committee may order a thorough investigation**. An **Investigation Unit set up specifically for that thorough investigation** by the President of the Ethics Committee on the proposal of the Compliance Officer, conducts each investigation. In this way, only those people designated and authorised to deal with them have access to the reports. The Compliance Officer coordinates the investigations.

The aim of the investigation is to analyse and verify the reality of the allegations disclosed in the report.

The investigation may include a documentary, accounting and/or electronic review or formal interviews with employees and/or stakeholders whose testimony is relevant to the investigation.



As a matter of principle, these interviews conducted as part of a thorough investigation are recorded in minutes. A copy is sent after the interview so that the interviewee can confirm the accurate transcription of the exchanges or produce corrections or additional information.

As part of the investigations carried out, SERIS may, in compliance with applicable legal requirements, have access to the computerised professional data of the persons involved or mentioned in the report, such as emails, data stored on the Group's IT infrastructures, in a business telephone or computer, etc.

These checks are carried out impartially and neutrally, taking into account all the factors that make it possible to assess the reality of the facts, for the benefit of both the person accused and the person who reported the incident, regardless of the persons involved or their hierarchical level.

They must not result in the collection of information by means that are unlawful, unfair or disproportionately prejudicial to the rights of the persons involved and to individual and collective freedoms.

When a law firm carries out the investigation, attorney-client privilege applies only to the relationship between the lawyers and SERIS. The person interviewed cannot therefore invoke it. SERIS may use any information or statement collected as part of the internal investigation, and in particular information collected during interviews.

If necessary, **preventive measures** are taken at the start of the investigation to ensure the protection of persons or property and to preserve the evidence needed to establish the facts reported.

Once these measures have been taken, the Case Manager in charge of the case will inform the persons involved or mentioned in the report in writing about the processing of their personal data under the whistleblowing system.

As a matter of principle, the people in charge of the internal investigation draw up an investigation report at the end of these checks.

The aim of the investigation report is to substantiate the facts in a factual report that objectively confirms or refutes the allegations referred to in the report.

### 3.4 What happens at the end of an internal investigation?

All first-level investigations reports establishing misconduct and all thorough investigations reports, regardless of their findings, are forwarded to the Compliance Officer and the President of the Ethics Committee, who convenes a meeting of the Ethics Committee to decide **on the action to be taken**.

Based on the conclusions of the investigation reports, which are communicated to it, **the Ethics Committee formalises its recommendations:**

- **dismissal of the** case if the facts are not proven, that is if the investigation does not establish the veracity of the alleged facts or if the evidence collected is insufficient.
- **action to be taken** if the facts are proven.

These actions can be:

- **internal remedial measures**, for example: reinforcing a process, raising awareness or training the employees concerned, reminding them of the applicable rules, communication action, etc.;
- a **breach of contract** with a third party (if the third party is involved);
- **disciplinary measures** ;
- **legal action**.

The Ethics Committee forwards its recommendations to the relevant management body for a decision, and enforcement of the decision is then entrusted to the department responsible for implementing the decision.

The Human Resources departments and line managers of the people involved are responsible for implementing the remedial plan decided by the relevant management body. This remediation plan may be individual or collective, and may take the form of training programmes, coaching, mediation or even the implementation of a disciplinary procedure that may go as far as dismissal.

## 3.5 To sum up





# 4

**Rights, duties and obligations  
of persons involved  
in an ethics report**



## 4. Rights, duties and obligations of persons involved in an ethics report

### 4.1 How is the confidentiality of information gathered in the context of a report protected?

**The principle of confidentiality is the cornerstone of the protection of individuals** under the whistleblowing system.

All persons called upon to process an ethics report are subject to a strict confidentiality obligation designed to **protect the identity of persons** involved in the report or in the investigation, as **witnesses, whistleblowers or alleged perpetrators**. Where necessary, these persons (Case Managers in particular) make a personal commitment by signing a formal confidentiality undertaking (regulated professionals bound by a professional obligation of confidentiality, such as attorney-client privilege for lawyers, for example, are not required to sign a specific confidentiality undertaking).

These people are required not to reveal any information to which they have had access (questions, answers, subjects dealt with, people involved, etc.). This requirement not only protects the reputation of all those involved, but also contributes to the smooth running of the investigation by avoiding any influence.

Beyond that, access to this information is strictly forbidden to people who are not authorised to know about it.

It should be noted that the Sapin II Act introduced an offence punishable by up to 2 years' imprisonment and a fine of up to €30,000 (€150,000 for legal entities) for disclosing the identity of the whistleblower or the persons to whom the report relates.

The protection of the data exchanged is simplified and strengthened when data is exchanged via the **SERISETHICS** platform.

Information identifying the whistleblower may only be disclosed with that person's consent. However, this restriction does not apply to the persons responsible for processing the report or the remedial plan identified at the end of the investigation.

In addition, information likely to identify the whistleblower may be communicated to the competent authorities, if SERIS is obliged to report the facts or if the Group has a legitimate interest in doing so. The whistleblower is then informed, unless this information could compromise the procedure in progress.

The information collected and processed as part of an internal investigation may include personal data. It is processed in accordance with the Group's personal data processing policy. The specific provisions relating to the protection of personal data in the context of the internal whistleblowing system are available on the **SERISETHICS** platform.

## 4.2 Is collaboration to an internal investigation mandatory?

The whistleblower, the alleged perpetrator and witnesses, the experts and other parties involved are expected to **cooperate fully and completely** and to provide, without delay or restriction, the facts, information or documents, in whatever form or on whatever medium, to the persons responsible for processing the report.

This cooperation includes honouring invitations to interview.

Although they are under no obligation to cooperate, their involvement is necessary for investigations to run smoothly and for the truth to be uncovered.

## 4.3 What information is passed on to the people involved?

### 4.3.1 Informing the whistleblower

The whistleblower is kept informed at every stage of the process.

Whistleblowers who choose to remain **anonymous** will only be informed of the follow-up to their report if they have made their report on the **SERISETHICS** platform and must therefore connect to the Secure Mailbox corresponding to their report.

**Within 7 days** of reporting, the whistleblower will receive **confirmation that his/her report has been received**.

Within **3 months** of receiving the report, the whistleblower will be informed in writing whether his/her report is admissible under this whistleblowing policy or not.

- **If the report is deemed not admissible under this policy:** the whistleblower is also informed of **the reasons why the report is not admissible**. In this case, the Case Manager in charge of analysing the admissibility of the report may forward it directly to the person responsible for dealing with such matter (HR, Risk Management, Communication, etc.); he/she will inform the whistleblower accordingly.
- **If the report is deemed admissible under this policy:** the whistleblower is informed on the **progress made in processing the report**, i.e. the measures planned or taken to assess the accuracy of the allegations.

**In the event of an admissible report, the whistleblower will also be informed in writing of the end of the investigations and the closure of the case**, as well as the main measures taken to remedy the situation, if any.

## 4.3.2 Informing the alleged perpetrator

In principle, any person involved in a report is informed if an analysis or ethical investigation is carried out.

This information is provided **after the admissibility check** of the report has been carried out, and may be delayed if there is a need to protect individuals or information useful to the ongoing analysis or investigation (for example to avoid any risk of destroying evidence).

Certain information relating to the report must also be shared with the accused person in order to give him/her the means to explain the facts in question.

The alleged perpetrator is also informed of the closure of the processing operation and, where applicable, of the main measures taken to remedy the situation.

The alleged perpetrator is informed in accordance with the regulations on the protection of personal data.

## 4.3.3 Informing witnesses

In principle, witnesses who have been interviewed or have collaborated in any way with an investigation are informed when the investigation is closed.

## 4.4 How is whistleblower protected against retaliation?

SERIS will not tolerate any retaliation against a person who has made a report or participated in the processing of a report.

The concept of "retaliation" refers to all unjustified and/or prejudicial measures taken against the whistleblower, facilitators, witnesses or any person connected with the whistleblower, because of the report.

Any whistleblower or any person who has provided information in the context of the processing of a report who believes that he or she is the subject of retaliation, including threats and attempts of retaliation for having made a report or participated in its processing, may report it to an authorised person, including via the **SERISETHICS** platform.

A follow-up may be carried out for the benefit of the whistleblower as well as facilitators, witnesses or other persons involved in the processing of the report, within a period of up to one year from the closure of the case in order to verify the absence of retaliation.

## 4.5 What are the sanctions in case of a breach of this whistleblowing policy?

In order to ensure the effectiveness of this whistleblowing policy and the protection of the persons involved in this policy, **sanctions, including termination of the contractual relationship, or legal action** may be taken in the event of:

- **Reports that are slanderous** or made in bad faith, or with the intention of obtaining direct financial compensation;
- Obstructing or attempting to **obstruct whistleblowing** or the processing of a report ;
- **Breach of the obligation of confidentiality** in connection with the receipt or processing of a report ;
- **Retaliation** or threats of retaliation, or any form of abusive procedure, against the whistleblower, facilitators and/or third parties linked to the whistleblower.

## 4.6 How is whistleblowing system monitored at Group level?

The Compliance Officer, covering all the reports received and processed over the past year, produces a fully anonymised report annually.

This report presents a quantitative and qualitative analysis of the data (in particular: types of subject matters reported, admissibility rates, types of action taken).

It is presented annually to the Ethics Committee and to the SERIS Group's governing bodies.

## 4.7 Are there any other ways of reporting?

As a matter of principle, whistleblowers are encouraged to use internal reporting channels in the first instance so that the situation can be remedied within the Group as effectively and quickly as possible, while providing the whistleblower with enhanced guarantees of confidentiality.

The whistleblower may nevertheless report the matter to an authorised external authority formally dedicated to receiving such report in his/her country.