SALOMON

# GUIDELINES FOR COLLECTING AND PROCESSING PROFESSIONAL ALERTS

*This procedure is established within the framework of Law No. 2016-1691 of December 9, 2016, known as the "Sapin 2 law" on transparency, the fight against corruption and the modernization of economic life, Law No. 2022-401 of March 21, 2022, to improve the protection of whistleblowers and the implementing decree n°2022-1284 of October 3, 2022.*

## Summary

## PREAMBLE

This procedure for collecting and processing professional alerts is set up within the Salomon SAS Company and is part of the Amer Sports Group global Whistleblowing Policy which applies to all employees of the Group.

The Amer Sports group takes the culture of trust and high business ethics very seriously. Our shared values support and guide our operations around the world.

Every Amer Sports employee is responsible for their own behavior, acting with integrity and observing the highest standards of business ethics.

The whistleblowing channels provide an opportunity to report suspicions of misconduct in confidence. There are different options for reporting, some of which allow reporting anonymously. The whistleblowing channels are an important tool to

- discourage illegal or unethical activity or business conduct that could disrupt the operations of the Group, damage its reputation or harm its relationships with employees or external stakeholders;
- foster compliance with laws and regulations as well as high business ethics within the Group; and
- ensure that reporters feel encouraged to report matters without the risk of subsequent victimization, discrimination or disadvantage when raising legitimate concerns.

## 1. SCOPE OF APPLICATION

### A. THE REPORT ISSUER

*"A whistleblower is a natural person who reports or discloses, without direct financial compensation and in good faith, information relating to a crime, offence, threat or harm to the public interest, a violation or an attempt to conceal a violation of an international commitment duly ratified or approved by France, of a unilateral act of an international organization made on the basis of such an undertaking, of European Union law, of the law or regulation. Where the information has not been obtained in the course of the professional activities referred to in I of Article 8, the whistleblower must have had personal knowledge of it». Article 6 of Law No. 2016-1691 of 9 December 2016.*

Thereby, the persons who may issue a report are:

1° Staff members, persons whose employment relationship has ended if they obtained the information in the course of that relationship, and individuals who applied for employment with the entity when the information was obtained as part of that application;

2° Shareholders, associates and holders of voting rights in the entity's general meeting;

3° Member of the administrative, management or supervisory body;

4° External and occasional employees;

5° Contractors of the entity, their subcontractors or, in the case of legal entities, members of the administrative, management or supervisory bodies of such contractors and subcontractors, as well as members of their staff.

## B. SUBJECT AND CONTENT OF THE REPORT

As specified in Article 6 of Law No. 2016-1691 of December 9, 2016, information that may be reported as an alert must concern situations that may constitute:

- A crime or an offence
- A threat or prejudice to the general interest
- A violation or an attempt to conceal a violation:
    - Of the law or of regulations,
    - Of an international commitment regularly ratified or approved by France,
    - Of a unilateral act of an international organization taken on the basis of such a commitment,
    - Of the law of the European Union.

Are excluded from the scope of the alert, the facts, information, or documents whatever their form or their support, which are covered by:

- National defense secrecy,
- Medical secrecy,
- The professional secrecy of the lawyer,
- The secrecy of the investigation or the judicial instruction.

It will be up to the whistleblower to transmit the necessary information and documents, whatever their form or their support to substantiate the alleged facts, as well as the elements allowing, if necessary, an exchange with the recipient of the alert.

Only the following data categories can be processed:

– identity, functions and contact details of the issuer of the professional alert;
– identity, functions and contact details of persons subject to an alert;
– identity, functions and contact details of the persons involved in collecting or processing the alert;
– reported facts;
– information gathered as part of the verification of the reported facts;
– report on the verification operations;
– action taken on the alert.

The facts gathered are strictly limited to the acts covered by the alert device.

The consideration of the professional alert is based only on data formulated in an objective manner, directly related to the perimeter of the alert device and strictly necessary to verify the alleged facts.

The formulations used to describe the nature of the reported facts reveal their presumed character.

### C. THE STATUS OF THE ISSUER OF THE REPORT

#### The protections

Under this device, whistleblowers enjoy civil and criminal protection and shall not be subject to disciplinary sanctions or retaliatory measures.

Whistleblowers are not liable under civil law for damages caused by their reporting or public disclosure as long as they had reasonable grounds to believe, when they did so, that the reporting or disclosure of such information was necessary to safeguard the interests in question.

Whistleblowers, as define by the law, benefit from the criminal irresponsibility under the article 122-9 of the penal code.

Failure to use this device may not result in any sanctions against staff members.

#### Sanctions

The abusive use of the device may expose the perpetrator to disciplinary action as well as prosecution.

The use of the device in good faith, even if the facts later prove inaccurate or give rise to no action, will not expose its author to any disciplinary sanction.

Any person who obstructs, in any way, the transmission of a report is punished by one year's imprisonment and a €15,000 fine.

## 2. THE INTERNAL REPORTING

### A. INTERNAL REPORTING CHANNELS

Two internal reporting channels are possible, one of them is anonymous.

If, despite the implementation of these exclusive channels, a report is received by an unauthorized person or service, it must be sent immediately to the persons listed below.
In cases of serious and imminent danger, or where there is a risk of reprisal or special circumstances that do not permit effective remedy of the facts reported, public disclosure may be used (see Section 3).

- Alternative 1: Reporting to the "whistleblowing" team:

The report can be sent by email to one of the "whistleblowing" team members, namely:

| | |
|---|---|
| Anna-Catherine Bénard-Lotz<br>Legal and Intellectual Property Director<br>anna-catherine.benard-lotz@amersports.com | Magali Clement<br>Chief People and Culture Officer<br>magali.clement@salomon.com |

The issuer of the professional alert must identify himself, but his identity is treated confidentially. The identity of the author cannot be disclosed without his consent.

The subject line of the email must be “Confidential – Occupational Alert”. The names of the persons or organizations concerned by the alert must not be mentioned in the subject line of the email.

The following four elements should be mentioned:

1. Subject of reporting
2. Date of facts or information
3. Place of occurrence of facts or information
4. The detailed description.

All documents supporting the alleged facts may be sent directly via the electronic email as attachments or as a shared link.

- Alternative 2: Anonymous reporting via a secure and confidential device

Reporting can be done anonymously via a secure and confidential device provided by an external partner, the “NAVEX”.
The link to this device is available on the Salomon intranet, Salomon.com, and Amer Sports website: https://amersports.ethicspoint.com

The report is made via a form available in several languages, including French and English, and which includes a list of information to complete online with the possibility of attaching documents.
Sending the completed form will generate the creation of a username and password on the screen, which must be saved securely, and which will allow anonymity to be maintained throughout the processing of the report.

## B. RECEIVING, PROCESSING AND CLOSING INTERNAL REPORTS

The internal reports are handled by the “Whistleblowing” team.

Upon receipt of the alert, a member of this team will send an acknowledgement of receipt of the report by email within seven working days from the receipt.
This acknowledgement of receipt shall be timestamped and shall summarize all the information and, if any, the attachments submitted as part of the report.

The person in charge of processing the report will verify, unless the report is anonymous, that all the conditions for exercising the right to alert are met (quality of the whistleblower, subject of the alert, good faith of the whistleblower, lack of direct financial compensation, etc.).

She may request any additional information from its issuer in order to assess the accuracy of its claims and will inform the issuer of the report of the reasons, if any, why its report does not meet the required conditions.

If the report is anonymous, it will be treated provided the following conditions are met:

1. the seriousness of the facts mentioned is established and the facts are sufficiently detailed;

2. the processing of this alert must be accompanied by special precautions, such as a prior examination by its first recipient of the opportunity of its diffusion within the framework of the device.

The person in charge of processing the report may arrange a one-on-one meeting with the whistleblower to exchange information.

She will then arrange a one-on-one conversation with the person who is the subject of the alert to:

- Inform them of the situation and gather their feelings and opinions
- Explain this device
- Provide a copy of the reporting procedure.

If necessary, other interviews, individual or collective, may be considered with the agreement of all.

A reasoned reply (information on the considered or taken measures to assess the accuracy of the allegations and, if necessary, to remedy the subject of the report and the reasons for it) will be forwarded to issuer of the report on the follow-up to the alert.
This response will be made within a reasonable time and at the latest within 3 months of the report (3 months from the acknowledgement of receipt of the report or, if there is no acknowledgement of receipt, 3 months from the expiry of the 7 business days following the report).

The issuer of the report will be informed in writing of the closure of the case when the allegations are inaccurate or unfounded, or when the report has become irrelevant.

## C. CONFIDENTIALITY AND DISSEMINATION OF INFORMATION

Reporting must be carried out with the utmost respect for the confidentiality and integrity of the persons affected by the said alert and the information transmitted.

The identity of the issuer of an alert and the persons concerned by the alert, as well as the information collected by all the recipient of the alert, shall be treated as confidential.

The person who is the subject of an alert may under no circumstances obtain communication from the person in charge of the processing, on the basis of his right of access, of information concerning the identity of the issuer of the alert.

Access to messages and information received through reporting channels is limited to those designated and authorized to process professional alerts. Their actions are recorded, and their treatment is confidential.
If necessary, individuals who can contribute their expertise may be included in the investigation process, with the consent of the issuer of the report in the event that their identity is disclosed. They can access relevant data and are also bound by confidentiality.
Access to information collected in connection with a report is prohibited to any other person not mentioned above.

Information that may identify the person implicated in a report may be disclosed once it has been established that the alert is well-founded.
Under the legal conditions, a transmission may be considered at the request of the judicial authority.

## 3. EXTERNAL REPORTING AND PUBLIC DISCLOSURE

### A. EXTERNAL REPORTING

Any whistleblower may also send an external report, either after having made an internal report under the conditions provided for in this procedure, or directly:

1. To the competent authority among those designated by decree no. 2022-1284 of October 3, 2022;
2. To the Defender of Rights, who directs him to the authorities best able to know about them;
3. To the judicial authority;
4. To an institution, body or agency of the European Union competent to collect information on violations falling within the scope of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019.

When the authority considers that the report does not fall within its competence, or that it also falls within the competence of other authorities, it shall immediately transmit it to the competent external authority or to the Defender of Rights, under conditions that ensure the integrity and confidentiality of the information it contains.
The issuer of the report will be informed of this transmission.

### B. PUBLIC DISCLOSURE

Any whistleblower may publicly disclose the serious facts of which he has knowledge:

1. After having made an external report, whether or not preceded by an internal report, without any appropriate action having been taken in response to that report within 3 months;
2. In case of serious and imminent danger;
3. In the particular case of information obtained by the whistleblower in the course of his professional activities, in the event of imminent or manifest danger to the general interest, in particular where there is an emergency situation or a risk of irreversible damage;
4. Or when the external report would create a risk of retaliation or would not effectively remedy the subject matter of the disclosure, due to the particular circumstances of the case, in particular if evidence may be concealed or destroyed or if the issuer of the report has serious grounds to believe that the authority receiving the report may be in a conflict of interest, in collusion with the author of the facts or involved in these facts.

When public disclosure is detrimental to the interests of national defense and security, the whistleblower may use this option only after having made an external report (see 1. above).

## 4. GDPR COMPLIANCE

This procedure is in accordance with the French data protection authority's (CNIL) framework adopted on July 18, 2019, concerning the processing of personal data intended for the implementation of a professional alert system.

## A. INFORMATION OF THE PEOPLE INVOLVED, INFORMATION OF THE EMPLOYEES AND DISPLAY

With regard to the principles of transparency and loyalty, it is the responsibility of the persons in charge of the processing of the alert inform the persons involved individually and collectively.
This information includes:

- the existence of the processing,
- its characteristics (in particular the intended purposes, the types of data likely to be included, the types of persons likely to issue or be the subject of the alert, the main stages of the procedure triggered by the alert, the duration of the data retention period, etc.),
- the entity responsible for the device,
- the alleged facts,
- the rights of the persons concerned.

It does not contain information about the identity of the issuer of the alert or that of third parties. However, when a disciplinary sanction or a litigation procedure is initiated following the alert in respect of the person subject to the alert, the latter may obtain disclosure of these elements under the rules of common law (rights of defense in particular).

The information of the person subject to an alert (e.g., witness, victim, alleged perpetrator) must be provided within a reasonable period of time, not exceeding one month, following the issuance of an alert.
This information may be deferred when it is likely to "seriously compromise the achievement of the purposes of said processing." This could be the case, for example, where the disclosure of such information to the person involved would seriously compromise the needs of the investigation, for example in the presence of a risk of destruction of evidence. The information must then be delivered as soon as the risk is eliminated.

This procedure will be presented to employee representatives and all employees, including external or casual employees.

The work council was consulted on this procedure.
A display will indicate the contact information of persons who can welcome and accompany reports.

## B. RIGHT TO ACCESS, TO RECTIFY AND TO ERASE DATA

In accordance with the law of January 6, 1978, as amended and the General Data Protection Regulation of 27 April 2016, known as «GDPR», the person responsible for processing the alert guarantees to all persons identified in the professional alert device the right to access the data concerning them and to ask, if they are inaccurate, incomplete, equivocal, or outdated, rectification, erasure or limitation of processing.

The exercise of the right to access must not allow the person exercising it to access personal data relating to other natural persons.
The right to rectification and erasure of data must be assessed with regard to the purpose of the processing. In particular, it must not allow retroactive modification of the elements contained in the alert or collected during its instruction.

Its exercise, when accepted, must not lead to the impossibility of reconstructing the chronology of any changes to important elements of the investigation.

This right can therefore only be exercised to correct factual data, the physical accuracy of which can be verified by the person in charge of the processing in support of evidence, without erasing or replacing the data, even erroneous, originally collected.

## C. RETENTION PERIOD FOR PERSONAL DATA

Personal data must only be kept in a form that allows the identification of individuals for the time strictly necessary to achieve the intended purposes. It is therefore with regard to the purpose that the retention period will be determined.

The duration of data retention or, when this is not possible, the criteria used to determine this duration are among the information that must be communicated to the persons involved.

Under these conditions, it is the responsibility of the person in charge of the processing to determine this duration prior to the achievement of the processing.

The data relating to an alert considered, as soon as it is collected by the person in charge of the processing, as not falling within the scope of the device are destroyed or anonymized without delay, after response to the issuer.

When no action is taken on an alert falling within the scope of the device, the data relating to this alert shall be destroyed or anonymized by the organization responsible for managing the alerts within two months of the closure of the verification operations.

Where disciplinary procedures or litigations are initiated against the person questioned or the author of an abusive alert, the data relating to the alert are kept by the person in charge of the processing of the alert until the end of the procedure or the prescription of appeals against the decision.

With the exception of cases where no follow-up is given to the alert, the data may be kept in the form of an intermediary archive for the purpose of ensuring the protection of the whistleblower or allowing the identification of continuing offences.

Regulations on the protection of personal data shall not apply, in particular regarding retention periods, to anonymous data, that is, those who can no longer be put in relation to one or more identified or identifiable natural persons.
The person in charge of the processing of the alert may retain the anonymized data without any time limit.
In this case, the organization concerned must guarantee the anonymization of the data on a permanent basis.