VIRBAC SIGNAL

-

WHISTLEBLOWING MANAGEMENT PROCEDURE

WHISTLEBLOWING PROCEDURE

1. OPERATING PRINCIPLES

1.1 DESCRIPTION AND LEGAL REFERENCES

Virbac is committed to full compliance with ethical rules and standards when carrying on and developing business activities. These rules are set out in the Group's code of conduct and anti-corruption policy.

This ethical and professional whistleblowing procedure (the "Whistleblowing Procedure") applies to the professional whistleblowing system as defined in this procedure and aims to ensure the proper application of the Virbac code of conduct and to protect employees and stakeholders who, in good faith, report a deviation from the law and our code of conduct and to ensure the best possible handling of alerts thus raised.

This procedure is directly in line with:

- the Sapin II law, n°2016-1691 of December 9, 2016, relating to transparency, combating corruption and modernizing economic life, as amended in particular by law n°2022-401 of March 21, 2022;
- European directive 2019/1937 of October 23, 2019, on the protection of persons reporting violations of European Union law;
- transposition law n°2022-401 of March 21, 2022, in France, aimed at improving the protection of whistleblowers, and implementing decree n°2022-1284 of October 3, 2022, relating to procedures for collecting and handling alerts raised by whistleblowers, establishing the list of external authorities authorized to receive alerts;
- the national legislation in this area applicable to our subsidiaries.

It allows persons who may raise an alert to exercise their right to raise an alert and to benefit from the whistleblower protection provided for by the aforementioned provisions.

The system for collecting and reporting compliance alerts complements but does not substitute the traditional channels of internal communication, according to the rules specific to each country, such as through line management and staff representative bodies.

Special precautions are provided by Virbac to supervise the handling of alerts received, in accordance with applicable laws and regulations, including deliberation n°2023-064 of July 6, 2023, adopting a reference document relating to the processing of personal data intended for the implementation of a whistleblowing system and amending deliberation n°2005-305 of December 8, 2005, relating to the single authorization of automated personal-data processing implemented within the framework of whistleblowing systems (AU-004) of the CNIL [*Commission Nationale Informatique et Liberté* (French Data Protection Authority)].

1.2 GOVERNANCE

1.2.1 ALERT CONTACTS

Alert Contacts are persons designated by the organization (at the Group level but also locally) as preferred contacts to receive whistleblower alerts and carry out the task entrusted to them and described below. The Alert Contact is subject to obligations of secrecy, confidentiality and impartiality in performing his/her task.

(A) ALERT CONTACT'S ROLE AND OBLIGATIONS

The Alert Contact's role includes:

- receiving whistleblower reports and acknowledging their receipt within seven (7) business days,
- reviewing the alert, in law and in fact, and issuing an opinion on the admissibility of the alert,
- if necessary, requesting any additional information from the whistleblower to assess the accuracy of the allegations made,
- informing the whistleblower of the admissibility of their report and of the actions contemplated to assess the truth of the alert and analyzing the situation reported,
- gathering the experts necessary to conduct the investigation, if an investigation is contemplated,
- issuing an opinion to the Business Ethics Committee on the analysis of the reported facts and on the follow-up to be given.

Each Alert Contact personally commits to act professionally and comply with the following obligations:

- an obligation of secrecy by refraining from disclosing any confidential information of which he/she may be aware when performing his/her task.
- an obligation of confidentiality in all whistleblowing procedures by protecting the identity of the whistleblower (when not anonymous); the identity of the persons mentioned in the report or subject to the complaint; and all information gathered during the handling of the alert. However, this information (with the exception of the identity of the whistleblower as such) may be communicated in a restricted and limited manner for the purposes of the investigation.
- a duty of impartiality: the Alert Contact acts professionally, without bias, and does not represent any particular interests when performing his/her task. During investigations, the Alert Contact ensures respect for the rights of accused employees, in particular the presumption of innocence and the right to privacy, and reminds any person necessarily involved in conducting the investigations to respect such rights. In the event of a conflict of interest or potential involvement in the reported case, the Alert Contact undertakes to act transparently and to immediately withdraw from the case while informing the Ethics Committee of the potential or proven conflict. The case will then be entrusted to another Group Alert Contact or designee for handling.

The Legal Compliance department ensures compliance with the above principles by all Alert Contacts.

(B) APPOINTMENT OF ALERT CONTACTS

ALERT CONTACTS are Group employees specially authorized to receive and handle alerts, appointed by the Compliance department and approved by the subsidiary director and the Group Ethics Committee.

⇒ At the Group level, particularly for alerts transmitted through the Virbac Signal platform at https://virbac.besignal.com, the appointed Group Alert Contacts who have access to the alert are:

- Group Legal Compliance director: Zahra Mouhoubi
- Group general counsel: Marie-Paule Porte
- Group Human Resources director: Francesca Cortella

⇒ In countries where Virbac has a subsidiary, the appointed Alert Contacts are:

- the compliance officer or the Alert Contact designated by the subsidiary's managing director and approved by the Legal Compliance director. The choice will be submitted beforehand to the Group Business Ethics Committee for an opinion. This position may, for example, be filled by the Legal director when this position exists in the subsidiary or by the person responsible for legal matters for the subsidiary; and
- If applicable, one or more HR Alert Contacts appointed by the Group Human Resources director for alerts related to human rights matters and whose appointment must be approved by the Group Business Ethics Committee.

Depending on the specific needs of an investigation, and in the event that the appointed Alert Contact position does not exist in an entity, only the Group Alert Contacts may appoint one or more *ad hoc* Alert Contacts, who will be bound by the same obligations as the Group Alert Contacts themselves. Under the supervision of Group coordinators, they may also, where circumstances warrant, assign investigations to specialized external professionals, who are bound – by contract or by law – by an obligation of confidentiality.

Any alert received by an appointed Alert Contact must immediately be brought to the attention of:

- the Group Legal Compliance director and, failing that, the Legal director:
  - either for the notification and monitoring of the actions implemented or for support, if necessary, regardless of how the alert is categorized (particularly to meet alert reporting obligations at the Group level),
  - or for the handling or supervision of actions concerning matters specifically under the responsibility of the Legal Compliance department, assisted by the Group functional director(s) who have the means and the legitimacy to support the actions to be carried out, particularly the internal investigation (for example, international sanctions).
- the Group Human Resources director: for human rights matters, which include discrimination, harassment, physical and/or verbal abuse, child labor, etc.

- the EHS director: for environmental, health and safety matters.

If the alert concerns unlawful practices other than those mentioned above, the alert is transmitted:

↳ to the Group Legal Compliance director, who will propose the Group functional director(s) with the means and legitimacy to conduct the investigation and whose appointment will be approved in the Business Ethics Committee informed during an *ad hoc* session.

1.2.2 Business Ethics Committee

A Business Ethics Committee (hereinafter "Ethics Committee") is set up at the Group level to oversee the effective operation of the system for receiving and handling alerts and the proper application of this procedure. It has the authority to propose any improvements to this system and this procedure.

In this regard, it has the authority to review the various alerts raised at any stage of the procedure and, if necessary, approve which alerts are to be handled first, as well as the means and actions to be implemented based on the situations submitted to it by the person responsible for handling the alert.

Based on the results and conclusions obtained from handling the alerts, it decides whether the cases reported need to be passed on to the company management and how they should be analyzed in order to consider what action should be taken if the alert is justified and reprehensible events or situations have been established.

Composition:

- Group Quality and Compliance director
- Group Legal Compliance director (main Group Alert Contact and acts as committee secretary)
- Group general counsel (Group Alert Contact)
- Group Human Resources director (Group Alert Contact)
- Group Chief financial officer (participation limited to matters categorized as fraud, corruption and influence peddling, competition)
- Group Corporate Sourcing director

Depending on the matters submitted to it, the Business Ethics Committee can also consult any expert it might decide to appoint.

Frequency of meetings:

- As many times as this will be necessary, depending on the alerts reported and the work to be carried out, and at the discretion of the Group Alert Contact in charge of the matter,
- and at least twice a year to review the proper functioning of the alert system.

The members of this committee undertake to respect the following principles and shall ensure that any person appointed by it or any person involved in the handling of alerts shall do likewise:

- the confidentiality of information relating to alerts raised,
- the protection of personal data according to the rules set out below, and
- the presumption of innocence when facts or situations are not proven,
- the right to defense of the persons implicated in the alerts raised.

1.3 The right to raise an alert and its scope

1.3.1 The right to raise an alert is the right of any person with a professional relationship with Virbac to report illegal behavior or behavior contrary to business ethics, or any serious breach of the general interest of which they are aware in the context of their professional activities with Virbac or of which they are personally aware.

1.3.2 The subject of the alert may be any information relating to a crime, an offense, a threat or harm to the general interest, a violation or attempt to conceal a violation of an international commitment duly ratified or approved by France or of a unilateral act of an international organization taken on the basis of such a commitment, European Union law, or the law or regulations in one of the countries in which Virbac operates through a local subsidiary.

1.3.3 For example, the alert may relate to any act (confirmed or suspected) that constitutes a violation of the rules regarding:

- Corruption and influence peddling
- Fraud, embezzlement, theft, money laundering
- Discrimination and harassment
- Human rights
- Threat or serious damage to the environment
- Occupational health and safety
- International sanctions, embargoes
- Anti-competitive practices
- Non-compliance with laws, regulations or the general interest

1.3.4 Acts, information and documents that fall under national defense secrecy, medical secrecy, professional secrecy and secrecy regarding judicial deliberations or judicial investigations or inquiries are excluded from the alert system.

1.3.5 Any situation that does not appear to comply with the provisions of the Virbac code of conduct, which is the reference document for the ethical conduct expected by the company, may be the subject of an alert.

1.3.6 The purpose of the alert is to inform the company about acts or conducts that are illegal or contrary to business ethics. Potential disputes between an employee and an employer (other than those falling within the scope defined in 1.3, such as personal grievances) are excluded from the scope of alerts as defined by law and will be declared inadmissible if reported using the whistleblowing system. These cases must be handled directly by the employer.

1.4 WHISTLEBLOWERS

1.4.1 Persons who can raise an alert are:

- Staff members of the Virbac group companies, persons whose employment relationship has ended when information was obtained regarding that relationship, persons who applied for employment within the Virbac group companies when information was obtained regarding that application,
- Shareholders, partners and holders of voting rights in the general meeting of companies,
- Members of any administrative, management or supervisory body,
- External and contingent workers,
- Co-contracting parties of the company concerned, their subcontractors or, for legal entities, the members of the administrative, management or supervisory body of those counterparties and subcontractors as well as the members of their staff.

1.4.2 A whistleblower benefiting from the protection system:

- is a natural person,
- acts in good faith,
- must not have received direct financial compensation,
- must have obtained the information in the course of their professional activities or, if this is not the case, have been personally aware of the facts reported.

1.4.3 The report must be made in "good faith," i.e.,

- by having the reasonable belief that the information disclosed was necessary to safeguard the interests in question, which means the whistleblower must not have been aware, at the time of the reporting or disclosure, that the facts reported or disclosed were erroneous.
- the report is made without any malicious intent or any search for personal profit, and the person making the report has good reason to believe that the allegation is true.

1.4.4 The report must be made "without direct financial compensation," i.e.,

- no direct financial compensation may be derived from the report, in other words,
- the whistleblower must not have received any remuneration of any kind for making the report.

1.4.5 Any person who deliberately makes false or misleading claims may be subject to disciplinary or legal action in accordance with applicable laws and regulations.

1.4.6 Persons who express themselves in good faith will not be subject to any disciplinary or legal action if their statements are subsequently found to be irrelevant.

2. SUBMITTING A REPORT (AN ALERT)

2.1 Internal employees of the organization may submit a report directly to one of the Group Alert Contacts available to receive and analyze the alerts or to a local Alert Contact if the organization has expressly appointed one, or directly on our Virbac Signal platform at:

https://virbac.besignal.com

Please note that this method of receiving and reporting alerts complements but does not substitute the traditional channels of internal communication, according to the rules specific to each country, etc., such as through line management and staff representative bodies.

2.2 Workers outside the organization and all other stakeholders can report via our Virbac Signal reporting platform accessible via our Corporate website and at https://virbac.besignal.com.

2.3 The complete system for receiving reports, to which this procedure applies, is described in article 5 "Alert system: receiving alerts."

3. ALERT CONTENT

3.1 The report must include any relevant factual element, information or documents to support the alert so that the report is as comprehensive, precise, detailed and documented as possible. In particular, the report must specify the date on which the acts took place and the identity of the persons involved when the whistleblower knows this information.

3.2 The whistleblower specifies the reasons for their personal knowledge of the facts and whether a third party has been informed of the same facts, either by the whistleblower or by other means.

3.3 The whistleblower is asked to provide any information that will allow the organization, while protecting the confidentiality of the whistleblower's identity, to contact the whistleblower (last name, first names, contact information) and discuss the alert.

3.4 As an exception, an anonymous alert may be handled provided that the seriousness of the facts mentioned is established and the factual elements are sufficiently detailed. Specific precautions will be taken when handling the alert, such as a prior review by its first recipient. The secure Virbac Signal alert system allows for anonymity and secure exchanges with an anonymous whistleblower. However, please be aware that it is more difficult and sometimes impossible to handle an anonymous report or establish whether the facts are well-founded particularly when the anonymous alert was raised by means of a letter, for example. The organization therefore recommends that the whistleblower identify him/herself: the investigation process is made easier when the whistleblower's identity is known so that discussions may take place with him/her, it being noted that the organization undertakes to maintain his/her confidentiality.

4. CONFIDENTIALITY AND PROCESSING OF PERSONAL DATA

4.1 All persons involved in handling an alert are reminded that they must apply the strictest confidentiality to the information gathered when handling the alert and to the personal data of those involved in the reported acts or situation, whether this concerns the whistleblowers themselves or any person reported or suspected of having committed reprehensible acts.

4.2 In this regard, communications concerning an alert between an Alert Contact (and/or any appointed Alert Contact) and the whistleblower will be carried out to the extent possible through the platform where the whistleblower may access information about the personal data processing performed in this specific context before using the system:

https://virbac.besignal.com

or, whenever necessary, through encrypted internal electronic messages to maintain the confidentiality of personal data.

4.3 Not using this messaging system, or using other means of communication, will not affect the potential admissibility of the alert or expose the whistleblower to sanctions. Access to the messaging system on the platform is reserved for the Alert Contacts and only for persons designated by them for alert handling or investigations.

4.4 If an alert is reported by mail, use of the double-envelope method is recommended: all the components of the alert are inserted in a closed envelope, referred to as the interior envelope, with the note **Confidential / Alert Contact** - which will itself be inserted in a second envelope to be sent to the head office in France at the following address: Virbac SA - Legal Compliance Department, to the attention of the Alert Contact, 13e rue – LID BP 27 06511 Carros Cedex France.

4.5 Only the personal data needed to handle and investigate the alert are collected and saved by the organization, namely:

4.5.1 the identity, functions and contact details

(i) of the whistleblower;
(ii) the persons who are the subject of the alert,

(iii) the persons involved, consulted or heard in the receipt or handling of the alert;
(iv) the facilitators and persons connected to the whistleblower;

4.5.2 the facts reported;
4.5.3 the information gathered to verify the facts reported;
4.5.4 a report of the verification operations;
4.5.5 the follow-up given to the alert.

This personal data is collected and processed to determine the admissibility of reports, verify the facts and take any necessary corrective measures. It also enables the organization to comply with its legal obligations (in particular under the "Sapin 2" law of December 9, 2016, and the law of March 27, 2017, relating to the duty of care) and to protect its legitimate interests (by complying with the law and the organization's ethical principles).

4.6 The right to access, rectify and object to the use of data may be exercised within the legal and regulatory framework by contacting the Alert Contact directly via the platform with the access codes that will have been given to the whistleblower, or directly or by sending their request by email to: compliance@virbac.com, indicating the alert references.

4.7 Under no circumstances can the person who is the subject of an alert obtain information about the whistleblower's identity from the controller.

4.8 In addition, the whistleblower agrees to keep confidential the information that has been disclosed to the entity for the purposes of handling the alert, including the personal data of the persons cited in the alert or throughout the handling procedure, in order to enable the entity to conduct the internal investigation while respecting the rights of the persons implicated, in particular the presumption of innocence and the right to privacy.

4.9 Any data relating to an alert that is considered to fall outside the scope of this procedure will be deleted or archived after informing the whistleblower, if it is possible to communicate with them, and after the organization has anonymized the data.

4.10 If no action is taken on an alert, the organization will anonymize the case so that nothing can identify its whistleblower and the persons concerned. This anonymization will be carried out no later than 6 months after the closure of all alert admissibility or verification operations.

4.11 When disciplinary proceedings or legal proceedings are initiated against one or more persons implicated by the alert, the data relating to the alert will be kept until the end of the procedure or the end of the time limit to appeal the decision taken.

4.12 The data relating to the alert may be kept for longer in intermediate archiving in the event of a legal obligation (for example, to meet accounting, social security or tax obligations), or for probative purposes in the event of any audit or dispute, or for the purpose of carrying out quality audits concerning the process for handling alerts.

5. ALERT SYSTEM: RECEIVING ALERTS

5.1 Alerts raised by employees of the organization can be received:

↳ either by the Group Alert Contacts (or so-called "main" Alert Contacts) when the alerts are raised through the Virbac Signal interface at: https://virbac.besignal.com, made available to employees and stakeholders to gather the main information needed to start the handling process.

- ↳ or by simple email to the Group's Legal Compliance department at one of the following addresses: compliance@virbac.com,
- ↳ or directly by one of the organization's Alert Contacts, if one has been appointed.

Alerts raised by external stakeholders are collected via the digital alert system: Virbac Signal, accessible from the Virbac group website.

5.2 If an employee wishes to report a violation (confirmed or suspected) to his/her manager or indirect line manager, the latter may tell them to send their report to the entity's designated Alert Contact, to a Group Alert Contact or, preferably, to use the existing system for this purpose, Virbac Signal.

5.3 If, however, the employee wishes to alert their manager directly or any other manager, the latter takes note of the alert and transmits the information gathered via the inbox at compliance@virbac.com.

5.4 It is also possible to request an appointment by telephone or video conference or an in-person meeting to make a report to an Alert Contact; such an appointment or meeting may be organized no later than twenty working days after receipt of the meeting request.

5.5 Regardless of the method chosen by the whistleblower, any alert received must be recorded in a register that is under the responsibility of the entity's appointed Alert Contact for local subsidiaries or the Group Alert Contact.

5.6 This register must contain the following information: the date and time of the alert received, identification of the whistleblower (first and last name, address, email and telephone number, unless anonymous, if permitted by law), his/her status (employee, volunteer, student, beneficiary, donor, partner, supplier, customer, etc.), his/her capacity (person involved or third party), the structure to which they belong (if appropriate), the course of events (date/time, location, description), the identity of the person(s) involved (specifying whether vulnerable persons are concerned), the identity of the person(s) implicated, and the identity of the person(s) or departments informed. The Virbac Signal alert system is the preferred tool for receiving and recording alerts and monitoring them.

5.7 A whistleblower may raise an alert anonymously if permitted by the law of the country in which they reside. However, he/she is encouraged not to raise an alert anonymously for greater efficiency in handling the alert, regardless of how the alert is transmitted.

5.8 Nevertheless, anonymous whistleblowing will be allowed by the Virbac Signal alert receipt interface at: https://virbac.besignal.com, which is the only means to exchange information via electronic messaging, if necessary.

5.9 The whistleblower will be given a username and password. In all cases, these usernames and passwords will allow the whistleblower to connect to the Virbac Signal platform later to provide additional information about the alert given, to communicate with the Alert Contact in charge of the case, and to obtain information about the follow-up given to their alert.

5.10 Whistleblowers should note that nothing can be done if they lose their username and password, due to the need to maintain the desired anonymity. This also means that there can be no communication with the whistleblower by another means.

6. ALERT HANDLING:

REPORT ADMISSIBILITY

6.1 The organization verifies, handles and analyzes alerts as soon as possible and while observing the confidential nature of the alert. The whistleblower is not asked to conduct his/her own investigation or to seek to establish the legal status of the reported facts.

6.2 The whistleblower is informed in writing of the receipt of his/her report within seven working days of receipt of the alert by the organization. This acknowledgment of receipt does not constitute admissibility of the alert. In addition, the entity is free to request additional information from the whistleblower.

6.3 The alert is examined for admissibility within a reasonable period of time, normally not exceeding 20 working days after receipt of the alert. The whistleblower is kept informed as to whether or not it is admissible. If the report is admissible, an investigation will be carried out to determine the truth of the facts reported.

6.3.1 However, the time periods may vary depending on the components of the alert.

6.4 If the report is declared inadmissible, it will be closed without follow-up after the whistleblower is informed, if the whistleblowing system chosen by the whistleblower allows this. The personal data of the alert will either be deleted from the entity's databases or anonymized at the end of the 3-month period after its closure.

The alert is declared inadmissible if:

- the alert received does not comply with the conditions set out in articles 1.3 and 1.4 of this procedure,
- despite the Alert Contact's attempt to contact the whistleblower for more information, the alert lacks clarity, relevance and supporting information for the Alert Contact in charge of handling to initiate a preliminary investigation.

HANDLING OF ADMISSIBLE REPORTS

6.5 In the event that the alert is declared admissible:

6.5.1 The Alert Contact in charge of handling the alert may launch a preliminary internal investigation, including an interview with the whistleblower if identified, the persons referred to or cited in the alert and their managers, by asking them to confirm or deny and/or to complete the information already gathered and/or to provide any supporting documentation that the interviewees may hold.

6.5.2 If, based on these elements:

(a) The situation reported proves not to exist, is not corroborated by information added to the initial alert, or is not reprehensible → the alert will be closed with no further action taken.

(b) The situation reported is qualified and recognized by all the parties involved, and the information corroborates the facts collected, adequate corrective measures and/or sanctions will be proposed to the Business Ethics Committee, which will approve or amend the proposed measures for discussion and final approval with the line-management authority in a position to implement them.

(c) The situation reported seems non-compliant without being factually established or recognized, but the information gathered suggests that it is probable and serious → initiation of an in-depth investigation.

6.6 The Alert Contact may call on internal or external experts while handling alerts and, more generally, use the various departments of the organization. The persons thus involved are required to comply with the provisions of this procedure and in particular the provisions of article 4.

IN-DEPTH INTERNAL INVESTIGATION

6.7 In addition to the stages of the preliminary internal investigation, there may be interviews with other people, during which they are asked to produce any supporting evidence they might have.

6.8 In addition, depending on the issue concerned, the company's resources may be used:

(a) Audit of access controls and badges,
(b) Audit of accounting entries and documents,
(c) Audit of operations recorded in the company's different systems and tools (such as company email accounts),
(d) Use of external service providers such as audit firms or lawyers, etc.

6.9 The whistleblower may be involved in the investigation process to verify the facts he/she has reported, provide additional information or be heard by the Alert Contact or any expert designated by the latter.

6.10 The whistleblower will be informed of the closure of the alert as well as any additional information that the organization deems appropriate to communicate concerning the action taken or not taken, subject to the preservation of the rights of the persons involved and the Group's interests.

INVESTIGATION FINDINGS

6.11 The Alert Contact in charge of handling the alert decides to close the investigation when he/she deems it appropriate. This decision must be ratified by the Business Ethics Committee, which may request further investigation if it considers this necessary.

6.12 When an internal investigation, even a preliminary one, has been initiated, the Alert Contact in charge of handling the alert submits his/her findings to the Business Ethics Committee based on the facts that have been established and how they have been classified. The Business Ethics Committee examines this information, hears the Alert Contact in charge of handling the alert and the persons involved if it so wishes, and decides on how to classify the situation or the facts as well as the possible actions it advises or recommends.

6.13 Its opinion is purely advisory and is forwarded for action to the competent managing body:

(a) the general management of Virbac, if reprehensible and particularly serious events or situations (or involving the management of the subsidiary in which they have taken place) are confirmed by the Business Ethics Committee (or if there is a difference of opinion on this point between the person in charge of handling the alert and the Business Ethics Committee)

(b) the management of the Group company concerned, if reprehensible events or situations are confirmed by the Business Ethics Committee, but the seriousness of these events or situations allows them to be handled at this level only.

6.14 Based on the events and situations concerned, these actions may include, at the discretion of the managing body and in accordance with applicable legal provisions:

(a) Amendments of the rules or internal procedures to prevent the recurrence of similar events and situations,

(b) Disciplinary action against the person or persons carrying out or participating in the reprehensible acts or situations, in accordance with the applicable rules of labor law,

(c) Legal proceedings

HANDLING ALERTS THAT MENTION OR REFER TO A PERSON NORMALLY INVOLVED IN HANDLING ALERTS ACCORDING TO THIS PROCEDURE

6.15 If a concern is raised in which the person or persons committing the acts reported or the witness or any person otherwise involved is one of the persons responsible for handling claims as per this procedure, then:

(a) If this person is an Alert Contact, then the acknowledgement and monitoring of the alert will have to be carried out by an Alert Contact other than the one referred to and appointed by the Business Ethics Committee,

(b) If this person ought to have been responsible for handling the alert, then the handling of this alert will have to be entrusted to any other competent person with the necessary handling means whom the Business Ethics Committee may designate,

(c) If this person is a member of the Business Ethics Committee, then this person must refrain from attending the Business Ethics Committee meetings that will deal with the alert involving/concerning him/her, and to which he/she will no longer be invited, unless he/she is called upon to provide his/her testimony to the other members of the Business Ethics Committee. In this case, this person will not be able to participate in any decisions that might be taken,

(d) If this person is a decision-maker who ought to have been involved in deciding what action to take concerning the alert, then this decision will be referred to the higher-level management body (or to the Virbac board of directors, if the Virbac chief executive officer is concerned).

In general, no stage of the handling of an alert and no investigation measure following an alert may be entrusted to a person referred to in this alert, whether this person is referred to as the person responsible for the acts, the witness, the victim or a person otherwise involved in the reported situation.

7. PROTECTION AGAINST RETALIATION

7.1 Direct or indirect retaliation by an employee of the entity or by the entity itself against a person who has in good faith reported a situation referred to in article 1.3 above or provided assistance to the teams responsible for investigating it will not be tolerated and may give rise to disciplinary action or prosecution.

7.2 Any employee or worker who believes that they have been the subject of retaliation for having reported or testified, in good faith, to facts constituting an offense or a crime of which they are aware in the course of their duties may report it to the Group Legal Compliance department.

7.3 Any misuse of the system, in particular in the form of slanderous reports (reporting information that is known to be totally or partially inaccurate) or reports made in bad faith may result in disciplinary sanctions and/or legal action against the perpetrator.

7.4 Any employee who hinders or hindered the transmission of an alert or who retaliates.d. against a whistleblower may be subject to disciplinary sanctions that could lead to dismissal for serious misconduct, and/or may be subject to legal action.

8. STATISTICAL MONITORING OF ALERTS

8.1 In order to be able to assess the effectiveness of the alert system, the Group Legal Compliance department and particularly the Legal Compliance director acting as Group Alert Contact, implements an annual statistical monitoring concerning the receipt, handling and follow-up given to alerts.

8.2 This annual statistical monitoring may show the number of alerts received by type, closed cases, cases that gave rise to or give rise to an investigation, the number and type of measures taken during and at the end of the investigation (precautionary measures, initiation of disciplinary or legal proceedings, sanctions imposed, etc.) and may be shared with the company's general management, its board of directors and its audit committee. Aggregate data may also be used during training or communication to employees.

8.3 The Group Legal Compliance director will ensure that this statistical monitoring and subsequent communications do not in any way affect the confidentiality referred to in article 4 above. In particular, she will refrain, as is the case for any person appointed to handle alerts, from any communication that could identify the persons involved in the situation that gave rise to an alert.

9. DISTRIBUTION

9.1 The organization will bring to the attention of its employees and workers the existence of their right to raise an alert, including, for example, through posting or notification.

10. EFFECTIVE DATE AND PUBLICATION OF THE PROCEDURE

10.1 This procedure amends the whistleblowing procedure that entered into force on June 1, 2021, and was the subject of consultation with the relevant staff representative bodies concerning the alert system.

10.2 This procedure comes into force on [XXXXXXXX].

10.3 This procedure applies to all subsidiaries of the Virbac group, insofar as its implementation at a particular subsidiary does not conflict with local public policy provisions applicable to that subsidiary.

11. CONTACT

11.1 For any questions relating to this Procedure, and the guarantees governing the right to raise an alert, internal employees or external workers of the organization are asked to contact the Legal Compliance department at compliance@virbac.com. Requests for information concerning the right to raise an alert will not be considered as a report falling within the scope of the system of this Procedure.