

Procedure for reporting wrongdoing and irregularities (Whistleblowing)

Date:	20/09/2023
Owner:	Legal LKQ RHIAG
Approved by:	Executive Management Team LKQ RHIAG
Latest revision:	20/09/2023

Summary

Procedure for reporting wrongdoing and irregularities (<i>Whistleblowing</i>)	1
1. Legislative sources and other related documents	2
2. Purpose and aim of the Procedure	2
3. Scope of application	3
4. Internal Signaling Channels	4
4.1 Internal reporting mode	4
4.2 Management of the internal reporting channel.....	4
5. External signaling channels	6
5.1 Possibility of external signaling.....	6
5.2 Management of the external reporting channel	6
6. Public Disclosure and Reporting to the Judicial Authority	9
6.1 Public Disclosure	9
6.2 Reporting to the Authority	9
7. Protections and Support Measures for the Reporting Person	10
7.1 Confidentiality	10
7.2 Privacy.....	11
7.3 Protection against Retaliation.....	11
7.4 Limitations of liability	12
8. Management of retaliatory notices by ANAC.....	13
9. Conservation.....	13
10. Sanctions.....	13
11. Information and Training	14

1. Legislative sources and other related documents

On March 15, 2023, Legislative Decree No. 24/2023 of "*Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019 on the protection of persons who report breaches of Union law and on provisions regarding the protection of persons who report breaches of national laws,*" effective March 30, 2023, was published in the Official Gazette (hereinafter "Decree").

The Decree reorders Italy's domestic regulatory system on whistleblowing in order to:

- Ensure the manifestation of freedom of expression and information, which includes the right to receive and communicate information;
- Identify the different ways of submitting reports, in written or oral form, through well-defined channels;
- be the useful tool to counter and prevent alleged violations accrued within the work environment of the Company;
- ensure the protection, in terms of confidentiality, privacy and protection from retaliation, of individuals who expose themselves with reports so that they feel more incentive to make reports of wrongdoing, or alleged wrongdoing, within the limits and in the manner indicated in the decree itself.

The National Anti-Corruption Authority (ANAC) intervened in support of the Decree and its interpretation by approving, in Resolution No. 311 of July 12, 2023, the "*Guidelines on the protection of persons who report violations of Union law and protection of persons who report violations of national regulatory provisions. Procedures for the submission and handling of external reports.*"

WHEREAS, prior to the Decree, the LKQ Group, of which our Company is a part, adopted a policy on whistleblowing, governed by the "*Speak Up Policy,*" with the primary objective of encouraging anyone to report alleged unlawful or inappropriate conduct with respect to company procedures and policies. By Company, in this Procedure, we mean Rhiag S.r.l., its Italian subsidiaries (ERA S.r.l., Motorparts S.r.l., Stahlgruber-B.M. S.r.l., and MD2 S.r.l.) as well as LKQ Italia S.r.l.

Without prejudice to the *Speak Up Policy*, in implementation of the Decree itself, it is therefore necessary to prepare a specific procedure on the operation of reporting channels (Legislative Decree No. 24/2023-art 5.) and with particular emphasis on the protections provided for the reporting person (hereinafter "Procedure").

2. Purpose and aim of the Procedure

The Procedure is intended to take up the concepts expressed in the *Speak Up Policy*, while also providing clear information on the procedures and prerequisites for making reports in compliance with the Decree, either using the communication channels set up by the company or through external reporting channels.

In addition to the reporting methods defined by the Decree (regulated below), the Company has other channels that are useful for this purpose, such as the possibility of directly contacting its manager, HR and Audit functions or the Supervisory Board.

It should be noted, however, that in the event of the use of alternative and different channels from those provided for in the Decree and the Procedure, the protection regime provided by the Decree itself will not be guaranteed, unless it is expressly manifested, by the person who reports, the willingness to want to benefit from the protections provided by the Decree and this document.

3. Scope of application

The Procedure is made available to, and for the protection of, all employees of the Company and any third party (by way of example: the intern, volunteer, customer, contractor, business partner, or service provider) (hereinafter the "Reporting Party") who deems it necessary to make a statement or report information about an alleged violation, accrued within the Company's work environment, in order to ensure that there is a thorough investigation and that appropriate corrective action is taken where necessary (hereinafter the "Reporting Party" or "Reporting").

The document is also addressed to all those individuals who assist the Whistleblower in the reporting process and who work within the same work environment (hereinafter "Facilitator"), such as a colleague in the same office as the Whistleblower.

Information on alleged violations¹ covers all those illegal conducts, behaviors, acts or omissions that harm the integrity of the Company and committed within the organization of the Company with which the Reporting Party has relations (hereinafter "Violations").

Information on Violations may also cover Violations not yet committed that the Reporter reasonably believes could become such based on concrete elements. The elements may also be irregularities and anomalies (symptomatic indices) that the Reporter believes could give rise to one of the Violations.

By way of example and without limitation, the Violations under the Decree consist of:

- Administrative, accounting, civil or criminal wrongdoing according to national laws;
- The predicate offenses for the application of Legislative Decree No. 231 of June 8, 2001, or violations of the "*Organization, Management and Control Model*" adopted by Rhiag S.r.l. and LKQ Italia S.r.l.
- Violations of European regulatory provisions (e.g., anti-money laundering prevention; product safety and compliance; transportation safety; environmental protection...)

It is important to point out that the report may also cover information about conduct aimed at concealing the violations noted above.

By way of example only, however, information on reportable or reportable violations is not included:

- mere irregularities that do not, however, constitute a factor that would lead the Reporting Officer to believe that Violations may result;

¹ Legislative Decree No. 24/2023 defines in Article 2 paragraph 1-a what is meant by a violation by listing the list of offenses.

- Disputes, claims, or demands related to an interest of a personal nature of the Whistleblower that pertain exclusively to his or her individual labor relations (for example: interpersonal conflicts between the Whistleblower and another worker);
- the patently unsubstantiated reports;
- information that is already totally in the public domain;
- information acquired on the basis of poorly reliable indiscretions or rumors (so-called rumors).

The Report should be as circumstantial as possible so that those who receive it can best handle it. Therefore, it is essential that they be clear:

- The circumstances of time and place under which the reported event occurred;
- description of the fact;
- the generalities or other elements that make it possible to identify the person to whom the facts that are the subject of the Report are attributed.

The Decree has provided for a diversified system of submission of Reports and specific reporting channels to which the protection regime provided by the Decree applies. The reporting channels are: i) Internal Reporting Channels; ii) External Reporting Channel (ANAC); iii) Public Disclosure; and iv) Reporting to the Judicial Authority.

4. Internal Signaling Channels

Internal reporting channels are created with the aim of encouraging Whistleblowers to contact, in the first instance, the Company directly. This ensures easier and more immediate acquisition of relevant information by those closest to the source of the violations, thereby ensuring more effective prevention and detection of the violations themselves, contributing to the Company's improvement.

4.1 Internal reporting mode

The tools and methods useful for making Reports, made available by the Company and available on the institutional website are:

- in written form through a portal, accessible, without the need for prior authentication, at the following link:
<https://secure.ethicspoint.com/domain/media/it/gui/52262/index.html>, including via *QR Code* found on posters posted on company premises;
- orally by calling the dedicated Italian phone number: 800 715 004.

4.2 Management of the internal reporting channel

The reporting portal and phone number are maintained by the independent provider *EthicsPoint (NAVEX Global, Inc.)*, which ensures the confidentiality of the identity of the Reporting Party, the person mentioned in the report, any Facilitator as well as the content of the report and related documentation.

EthicsPoint, upon receipt of the Report, will forward it to the Company. The Whistleblower, if he or she wishes, may also make a Report completely anonymously.

Following the submission of the report through the portal, or upon completion of the call, a unique reporting code will be created and assigned to the reporter. This code, along with a chosen *password*, can be used after 5-6 working days to access the platform or by calling the phone number directly. In these ways, the Reporter will be able to ascertain the correct receipt of the report and will be able to send additional information about the report or check for comments, questions, and requests to supplement the information.

Subsequent management of the reporting channel is entrusted to the Company's *Legal and Compliance* Team (hereinafter "Team"), with personnel specifically trained and authorized for its management. The Team, specifically, performs the following activities:

- accesses the portal, using two-factor authentication, so as to view the Report;
- Appoints possible investigators: pre-appointed and trained individuals who can support the Team in the investigation inherent in the Report;
- assesses, independently or with the support of the Investigators, the existence of the essential requirements of the Report referred to in Section 3 above so as to verify its admissibility and be able to grant the Reporting Party all the protections provided;
- initiates an internal preliminary investigation phase on the reported facts so as to assess the existence of the same; if not, dismissal of the Report will be ordered with adequate justification;
- Maintains interlocutions, including anonymously, with the Reporting Officer, including asking the Reporting Officer for clarifications, documents and additional information. This activity is carried out through the portal (in case of anonymous reports) or also in person;
- acquires acts and documents from other offices, availing itself of their support, and involves third persons through hearings and other requests, always taking care that the protection of the confidentiality of the Whistleblower and the reported person is not compromised;
- diligently follows up on reports received about the outcome of the investigative activity and any measures to be taken;
- addresses internal organs and functions or external institutions, each according to its competencies;
- provides feedback to the Reporting Party within 3 (three) months from the date of the Reporting. It should be noted that the feedback may also be merely interlocutory, since information may be communicated regarding the progress of the investigation and the activities undertaken or to be undertaken. At the end of the preliminary investigation, the results must in any case be communicated to the Reporting Party
- makes available useful information regarding the internal reporting channels and the external one managed by ANAC, in a clear and easily accessible form. This information is made available within the Company's institutional website, on the intranet and with posters posted in workplaces.

We also point out that, where the report concerns a possible violation of Model 231 (adopted by Rhiag S.r.l. and LKQ Italia S.r.l.) or unlawful conduct relevant under Legislative Decree 231/01, the

Team will promptly send an information flow to the Supervisory Board of the aforementioned companies, guaranteeing the protection regime for reports provided for by the Decree itself.

It should be noted that, if the internal report is submitted to a person other than the above-mentioned person (e.g., the hierarchical superior) and where the *Whistleblower* expressly declares that he/she wishes to benefit from the *Whistleblowing* protections provided by the Decree or, such willingness can be inferred from the report or from conclusive behavior, the report is considered a "*Whistleblowing Report*." The same will then be transmitted, within 7 (seven) days of its receipt, to the *Legal and Compliance* Team giving simultaneous notice of its transmission to the reporting person. Otherwise, if the Whistleblower does not expressly state that he/she wishes to benefit from the protections provided by the Decree, or said willingness cannot be inferred from the report, said report shall be considered as an ordinary report, therefore not a *Whistleblowing report*.

5. External signaling channels

5.1 Possibility of external signaling

The Whistleblower, in addition to the above-mentioned cases of internal reporting, may use an external reporting channel than those provided by the Company. This mode of reporting can be used only if:

- the Whistleblower has already made an internal report in the manner defined in point 4 above and the report has not been followed up by the Team. For example, in the case where the Team has not undertaken any of the activities referred to in point 4.2 above within the timeframe stipulated in the Decree;
- the Whistleblower has reasonable grounds to believe that if he or she made an internal report, it would not be effectively followed up. For example, there is well-founded concern that evidence of wrongful conduct has been concealed or destroyed;
- the Whistleblower has reasonable grounds to believe that the report itself may result in the risk of retaliation. For example, the case where a Whistleblower has already been presented with the possibility that he or she will be prejudiced if he or she reports;
- the reporting person has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest. For example, the case where the violation clearly requires urgent action by a public authority to safeguard an interest vested in the public such as health, safety or environmental protection.

5.2 Management of the external reporting channel

ANAC has made available a specific external reporting channel that guarantees, including through the use of encryption tools, the confidentiality of the identity of the Whistleblower, the person mentioned in the report, possibly the Facilitator, as well as the content of the report and related documentation.

As a preliminary step, ANAC makes use of specifically trained staff from the Office for the Supervision of *Whistleblowers'* Reports (hereinafter "UWHIB"). Only reports submitted by the Whistleblower will be taken into consideration, and therefore reports submitted by other individuals, including representatives of labor organizations acting on behalf of the organization itself, will not be

considered, as the institution of *Whistleblowing* is directed to the protection of the individual natural person acting on his or her own behalf. In the latter case, the reports are archived and, if related to matters within ANAC's jurisdiction, are treated as ordinary reports.

These kinds of reports may be made:

1. In writing via ANAC platform:
 - accessible via browser at the following Link:
<https://whistleblowing.anticorruzione.it/#/>;
 - which allows the identification of each report received by assigning a unique progressive code;
 - which allows for the completion, submission and receipt of the report form, management of the investigation and possible forwarding to other competent authorities;
 - which allows the Reporter to access the appropriate area of the platform to enter the report without prior authentication. In this area, the Reporter views the reporting form to be filled out and submitted. The form includes a special "Identity" section that the reporter must fill out to sign the report. The data entered in this section, useful for its unique identification, are subject to obscuration and therefore not accessible to the members of the office that will deal with the investigation unless explicit authorization to access upon reasoned request.
 - allows the reporter to monitor the progress of the process initiated as a result of the Report, integrate it and dialogue (anonymously and securely) with ANAC by accessing the platform through the use of a unique identification code provided to the reporter at the outcome of the submission of the Report.
 - allows the reporter to access his or her report for up to 5 (five) years following the date the file is closed by ANAC.
2. Orally through a telephone service with an operator who captures the report and enters it on the ANAC platform along with the audio file recording of the phone call.
The operator, upon completion of the entry of the report, acquires from the ANAC platform the unique 16-character alphanumeric identification code (key code) with which the reporter will first log in.
3. At the request of the reporting person, through a face-to-face meeting set within a reasonable time.
This type of report is captured through an operator who enters the report into the computer platform, similar to the oral reports described above

Upon acquiring the report, ANAC shall serve a notice of receipt of the report to the person concerned within 7 (seven) days, unless explicitly refused by the Reporting Party or the case where ANAC considers that the notice may prejudice the protection of the confidentiality of the Reporting Party.

ANAC will then verify that the conditions for making an external report (as listed in 5.1 above) are met, and where no conditions are met, the report will be dismissed.

Otherwise, ANAC will assess the eligibility requirements, which are:

1. manifest groundlessness due to the absence of factual elements attributable to the violations (e.g.: reports marked by predominantly personal issues);
2. manifest lack of the legal prerequisites for the exercise of ANAC supervisory powers, including the absence of the prerequisites for making the report;
3. Manifest incompetence of ANAC on the reported issues;
4. established generic content of the wrongdoing report such that the facts cannot be understood;
5. Production of only documentation in the absence of reporting misconduct;
6. Lack of data that constitute essential elements of the wrongdoing report;
7. Existence of minor violations.

In the cases referred to in numbers 4 and 6, ANAC may request additional elements from the Reporting Officer through a dedicated channel.

The UWHIB properly follows up on the reports received through the activities outlined below:

- outside cases of inadmissibility, the UWHIB forwards the report of wrongdoing to the relevant supervisory offices, which will carry out the investigative activities;
- if the report relates to unlawful acts that are relevant from a criminal or erarial point of view, the UWHIB archives it since it does not fall under ANAC's jurisdiction and orders its immediate transmission to the competent judicial authority, pointing out that it is a *Whistleblowing* report in whose management process, therefore, every precaution must be taken to ensure compliance with the provisions of the regulations.
- if the Report relates to violations that do not fall within the objective scope of ANAC's intervention, but rather within the competence of another administrative authority (by way of example only, the Civil Service Inspectorate, AGCM) or of an institution, body, or organ of the European Union, the UWHIB orders it to be archived because it is inadmissible and will be forwarded to the appropriate person, taking care to indicate that it is a *Whistleblowing* Report and that therefore all necessary precautions must be taken in terms of confidentiality protection and processing of personal data.

In any case, however, the UWHIB shall provide feedback to the Reporting Party within 3 (three) months or, if there are justified and substantiated reasons, 6 (six) months from the date of notice of receipt of the external report or, in the absence of such notice, from the expiration of 7 (seven) days from receipt.

It should be noted that the external report submitted to a subject other than ANAC will be transmitted to the latter, within 7 (seven) days from the date of its receipt, giving simultaneous notice of the transmission to the Whistleblower. The same applies to external reports mistakenly submitted to a subject other than ANAC that it believes to be competent, which must be transmitted to the latter where the reporter expressly states that he or she wishes to benefit from the protections provided by the Decree.

Such reports are considered *Whistleblowing* and the entity that received them will process them exclusively for the management of the investigation. On the other hand, in the event that the report is forwarded to an entity other than ANAC and the reporter does not expressly state that he or she wishes to benefit from *Whistleblowing* protections, said report is considered an ordinary report.

ANAC has started the process of evolving the IT platform in order to implement the functionality to the fullest. The new features will be made available to users gradually. For any further information regarding the ANAC Whistleblowing channel, please refer to the specific section at: [Whistleblowing - www.anticorruzione.it](http://www.anticorruzione.it).

6. Public Disclosure and Reporting to the Judicial Authority

The Decree introduces two other residual modes of Reporting: Public Disclosure and Reporting to the Judicial Authority.

6.1 Public Disclosure

Public disclosure consists of putting information about violations in the public domain (hereinafter "Disclosure"). This activity can be done by the Reporting Party through print media, electronic media, *social media*, and in general means of dissemination capable of reaching a large number of people.

As with the external reporting channel, there are specific conditions to the use of this modality for Disclosure. It should be noted that in the event of the existence of these cases (listed below) the Whistleblower will be guaranteed the regime of protection and safeguards provided by the Decree. The conditions for proceeding with the Disclosure are:

- an internal report has already been made without any response, and the Complainant then also made an external report to ANAC, which, in turn, did not respond in time;
- the Complainant has since the beginning made an external report to ANAC without receiving a response;
- The Whistleblower has reasonable grounds to believe that the external report may carry the risk of retaliation or may not be effectively followed up;
- the Complainant believes, with good reason and based on concrete circumstances, that the violation may pose an imminent or obvious danger to the public interest.

It is intended to clarify that if the Whistleblower voluntarily discloses his or her identity, confidentiality will not be guaranteed, without prejudice to all other forms of protection provided by the Decree.

Where, on the other hand, the Disclosure is made using, for example, a pseudonym that does not allow for the identification of the discloser, the Disclosure will be treated in the same way as an anonymous report and will be recorded by ANAC, for preservation purposes, to ensure that the Whistleblower, if his or her identity is subsequently disclosed, will be afforded the protections provided in the event that he or she suffers retaliation.

6.2 Reporting to the Authority

Protected persons are also granted the opportunity to approach judicial authorities so as to file a report of unlawful conduct. The offices of these authorities will abide by the same rules on the protection of confidentiality and the content of reports as provided for in the Decree.

7. Protections and Support Measures for the Reporting Person

The Whistleblower can rely on a system of protections that, as anticipated, also extends to parties other than the Whistleblower who, by reason of their role in the reporting process, could be recipients of retaliation.

The protection system includes:

- The protection of the confidentiality and privacy of the Whistleblower, Facilitator, the person involved and the persons mentioned in the Report, Disclosure or Complaint made;
- Protection from retaliation by reason of the Reporting, Disclosure or Complaint made;
- Limitations of liability with respect to the disclosure and dissemination of certain categories of information.

7.1 Confidentiality

The protection of the confidentiality of the Whistleblower is ensured by adopting appropriate ways of handling the Report, Disclosure or Whistleblowing and which enable the identity of the Whistleblower, the content of the report and the related documentation to be protected and kept confidential.

Confidentiality will also be guaranteed:

- To the person reported;
- to the person to whom the violation is attributed in the public disclosure;
- to the Facilitator, both in terms of identity and with reference to the activity in which the assistance takes place;
- to persons other than the person reported, but nevertheless implicated because they are mentioned in the Report or Disclosure (think, for example, of persons named as witnesses).

Compliance with the obligation of confidentiality will be ensured during all stages of the Reporting process, until the conclusion of the proceedings initiated on account of the Reporting, including the transfer of Reports to the competent authorities.

The identity of the Whistleblower, and any other information from which the identity may be inferred, directly or indirectly, may not be disclosed, without the Whistleblower's express consent, to persons other than those competent to receive or act upon Reports.

In order to ensure the utmost caution, the Team or in general the persons responsible for following up on reports are properly trained in order to avoid the undue circulation of confidential information, not only externally but also within the Company.

Confidential information will therefore be treated with the utmost caution first and foremost with the obscuring of personal data relating to the Reporting Party and other persons whose identity must remain confidential if, for investigative reasons, other persons must also be made aware of the content of the Reporting and/or the documentation attached to it.

An exception to this duty of confidentiality of the persons involved in or mentioned in the report is when the reports are reported to the judicial authorities.

With specific reference to Disclosure, confidentiality protection does not apply where the reporting person has intentionally disclosed his or her identity through, for example, *web* platforms or *social media*. The same applies in the event that the person directly contacts a journalist. In this case, in

fact, the rules on journalists' professional secrecy, with reference to the source of the news, remain unaffected.

7.2 Privacy

The processing of personal data related to the receipt and handling of internal reports is carried out by the Company as the Data Controller, in accordance with the principles of Articles 5 and 25 of Regulation (EU) 2016/679 (GDPR). This type of protection is also provided not only to the Whistleblower but also to the other parties to whom confidentiality protection applies (the Facilitator, the person involved and the person mentioned in the report) as they are all to be considered as "data subjects" of the processing of personal data according to GDPR.

The independent provider *EthicsPoint (NAVEX Global, Inc.)*, operator of the reporting platform is to be regarded as the Data Processor within the meaning of Article 28 of the GDPR.

On the other hand, the Company has identified individuals for the processing of Reports who are expressly authorized and who receive adequate and specific professional training aimed at increasing their specialized skills, including in the field of personal data protection regulations.

It should be noted that both the person involved and the person mentioned in the Report, with reference to their personal data processed in the context of the Report, Disclosure or Complaint, cannot exercise - for as long as and to the extent that this constitutes a necessary and proportionate measure - the rights that Regulation (EU) 2016/679 normally grants to data subjects (the right of access to personal data, the right to rectification, the right to obtain erasure or so-called right to be forgotten, the right to restriction of processing, the right to portability of personal data and the right to object to processing). The exercise of these rights could in fact result in actual and concrete prejudice to the protection of the confidentiality of the identity of the Reporting Person. In such cases, therefore, the reported person or the person mentioned in the report is also precluded from the possibility, where they believe that the processing that concerns them violates the aforementioned rights, of approaching the Data Controller and, in the absence of a response from the latter, of lodging a complaint with the Data Protection Authority.

7.3 Protection against Retaliation

The Whistleblower is protected from any kind of retaliation he or she believes he or she may have suffered as a result of the Report, Complaint or Disclosure made.

Retaliation can consist of both acts or measures, as well as conduct or omissions that occur in the work context and cause harm to the protected individuals. Retaliation also covers instances where it is only "attempted" or "threatened" (e.g., the prospect of dismissal or change of job description; non-renewal or early termination of a fixed-term employment contract; early termination or cancellation of a contract for the supply of goods or services).

Alleged retaliation must be reported exclusively to ANAC; in doing so, evidence must necessarily be provided from which the existence of the retaliatory threat or attempt can be inferred. The person accused of attempting the retaliation or threat will then have to prove that these facts are unrelated to the Reporting, Complaint or Disclosure.

There are certain criteria necessary in order to enjoy protection from retaliation:

- the Whistleblower made Reports, Public Disclosures, or Complaints, based on a reasonable belief that they were true (that a wrongdoing was about to occur, for example) regardless of whether those facts may later be determined to be incorrect.

Thus, protection also applies to the person who has reported, made Disclosures or complaints while being uncertain of the actual occurrence of the facts reported or denounced, the identity of the author thereof, or even reporting inaccurate facts due to genuine error;

- Reporting or other methods must be carried out in compliance with this Procedure and the Decree;
- there must be a close connection between the Reporting, (or the other modalities) and the retaliation suffered directly or indirectly, by the reporting or whistleblowing person.

This type of protection is guaranteed, as long as the above conditions are met, not only to the Whistleblower, but also to other individuals who may suffer retaliation because of their role in the Whistleblowing process and/or their particular relationship with the Whistleblower.

ANAC, once it receives the report on retaliation, initially assesses the link between the Report, Complaint or Disclosure and the distorting intent.

As previously mentioned, the Whistleblower will only have to prove that he or she made a Report, Disclosure, or Complaint and was retaliated against. It will then be the person accused of having carried out the retaliation who will have to prove the lack of connection between the retaliation and the Report.

Thus, for the Whistleblower, the harm is presumed and does not have to be proven by the Whistleblower himself; beware, however, that this benefit applies only to the Whistleblower and not to individuals who claim to have suffered retaliation by reason of their connection with the Whistleblower.

In the event that there is an anonymous report and, the Reporting Party subsequently identified, notifies ANAC that he or she has suffered retaliation, he or she may benefit from the protection that the decree guarantees against retaliatory measures.

7.4 Limitations of liability

In addition to the protections outlined above, accorded to the Whistleblower, Whistleblower or those who make a Disclosure, there are certain limitations of liability in cases where there is disclosure and dissemination of certain categories of information (for example: disclosures of information related to copyright protection, personal data protection...).

In order to obtain a limitation of liability, whether criminal, civil, or administrative, 2 conditions must be met:

- the Whistleblower, Whistleblower, or Discloser believes that the disclosure of this information is essential for the purpose of bringing out the violation, excluding those cases of violations to be considered unnecessary;
- Having made the report in compliance with the conditions stipulated in the Decree to benefit from protection from retaliation.

However, where the acquisition of or access to the information or documents in question has been obtained by committing a crime, such as abusive access or an act of hacking, the exclusion of liability does not operate, but criminal liability and any other liability, including civil, administrative and disciplinary liability, remains unaffected.

8. Management of retaliatory notices by ANAC

As previously mentioned, the reporting of retaliation suffered, referred to in Section 7.3 above, is entrusted to the external channel provided by ANAC.

ANAC then has the task of ascertaining that the retaliation is consequent to the reporting of wrongdoing and, if so, applying the sanction provided by the Legislature.

In the case of a retaliatory communication, the UWHIB first proceeds to verify the eligibility requirements. The communication is deemed inadmissible if:

- There is a lack of appropriate factual evidence to justify a finding of retaliation;
- there is no legal basis for the exercise of ANAC's powers;
- there is an "emulative" purpose of the reporter, such as acting in bad faith with a different end goal than reporting the retaliatory act;
- the communication has too general a content to allow understanding of the facts;
- Lack of essential data to make the communication or transmission of only documentation.

The author of the communication shall be promptly informed of the initiation of the proceeding, its outcome and conclusion.

Where it appears necessary to acquire additional information or documents, ANAC may summon those in possession of them to a hearing or send them a request for supplementary documentation with the assignment of a deadline within which to provide feedback.

The proceedings conducted by ANAC conclude with the adoption of a dismissal order or, where "retaliation" is established, with a penalty order (from 10,000 to 50,000 euros) against the person responsible for it.

9. Conservation

The Reports and related documentation shall be kept for as long as necessary for the processing of the Report itself and in any case no longer than 5 (five) years from the date of the communication of the final outcome of the reporting procedure, in compliance with confidentiality obligations and the principle of Article 5(1)(e) of Regulation (EU) 2016/679.

10. Sanctions

ANAC identifies several cases subject to sanctions. The following administrative pecuniary sanctions may be applied by ANAC itself:

- 10,000 to 50,000 euros when it determines that the individual identified as responsible has committed retaliation;
- 10,000 to 50,000 euros when it determines that the natural person identified as responsible obstructed the report or attempted to obstruct it;
- 10,000 to 50,000 euros when it finds that the natural person identified as responsible has violated the obligation of confidentiality. Penalties applicable by the Data Protection Authority remain unaffected;

- 10,000 to 50,000 euros when it ascertains that reporting channels have not been established, in which case the governing body is considered responsible in both public and private sector entities;
- 10,000 to 50,000 euros when it determines that procedures for making and handling reports have not been adopted or that the adoption of such procedures does not comply with the provisions of the Decree; in this case, the governing body is considered responsible in both public and private sector entities;
- 10,000 to 50,000 euros when it determines that the activity of verification and analysis of the reports received was not carried out; in this case the manager of the reports is considered responsible;
- 500 to 2,500 euros, when it is established, also by a judgment of first instance, that the Reporter is liable for defamation or slander in cases of malice or gross negligence, unless the same has already been convicted, also at first instance, for the crimes of defamation or slander or otherwise for the same crimes committed with the report to the judicial authority.

For more details on the process of individual sanction proceedings, please refer to the appropriate Sanction Regulations that ANAC will make available.

11. Information and Training

Information on this Procedure is made accessible and available to all, made easily visible in workplaces and also published in a dedicated section of the company website and, for employees, on the intranet.

Information on the Procedure is also made available when hiring an employee.

Training on *Whistleblowing* and, in general, on the provisions of this Procedure, is, in addition, included in the *Compliance program* provided by the Company.