PROCEDURE

Protection of persons who report breaches of Union law and violations of national laws, which come to their attention in a work context ('whistleblowing')

Legislative Decree 24/2023

ANNEXES

ANNEX 1

Description of internal channel(s) and security measures

Suedwolle Group Italia SpA, part of the Suedwolle Group takes its responsibilities very seriously, particularly with regard to human rights and environmental aspects. In order to implement the Whistleblower Protection Act, the company has implemented the following measures as part of the whistleblowing procedure.
Employees, suppliers, representatives, and subcontractors (hereinafter jointly referred to as "business partners") may report violations of the Suedwolle Group Code of Conduct at compliance@suedwollegroup.com.
All of our business partners will be informed of the wrongdoing reporting procedure and its confidential nature.
In addition to the above contact option, Suedwolle Group and consequently Suedwolle Group Italia SpA has appointed an external manager for the handling of wrongful reports.
The office can be reached as follows:

Baker Tilly Rechtsanwaltsgesellschaft mbH
Nymphenburger Str. 3b
80335 München
Germany
Telephone: +49 89 55066-525
E-Mail: ombudsservice.swg@bakertilly.de

The reasons for this choice are as follows:
Reports:
- e-mail: ombudsservice.swg@bakertilly.de
- via telephone: 49 89 55066-525
-
Baker Tilly Rechtsanwaltsgesellschaft mbH
Nymphenburger Str. 3b
80335 München
Germany

All reports to the Office are covered by current legislation regarding confidentiality and anonymity of the reporter (identity is not disclosed).
Reports concern any illegal behavior that has a business connection to the Suedwolle Group or does not comply with internal company guidelines. However, this must not include allegations against the judgment. In case of doubt, the Office named above is available to discuss what falls within the scope of the report.
The German external manager is bound by client confidentiality, thus ensuring that anonymous reports can be made. In addition, the group-wide goal is to minimize the different reporting channels for the Südwolle Group's European subsidiaries through an external manager-lawyer
The following additional methods are also provided:
- oral communication (including voice messaging) by contacting the following telephone number: **49 89 55066-525**

- at the request of the reporting person, by means of a face-to-face meeting with the person authorized to handle reports, set within a reasonable period of time

The main security measures, which guard the channel are shown in Annex 1. These measures ensure the confidentiality of the identity of the reporting person, the person involved and the person otherwise mentioned in the report, as well as the content of the report and related documentation.

As required by legislation (Article 4 of Legislative Decree 24/2023), the most nationally representative trade unions were heard before activation. This fulfillment took place in the following ways:

X informational with communication: departmental meetings, e-mail, uploading procedure and information Inaz employee portal, shortly uploading material on the website www.suedwollegroup.com/swgi

ANNEX 2

Communication RSA/RSU or OO.SS.

or
Spett.
OO.SS:
……

Subject: Reporting offences (Legislative Decree 24/2023)

WHEREAS:

a. Legislative Decree 24/2023 regulated, in implementation of the EU Directive 2019/1937, the reporting of wrongdoing within public and private entities (so-called whistleblowing)

b. Article 4 of the aforementioned Legislative Decree 24/2023 provides that the obliged parties must activate, their own "internal" reporting channels, which guarantee the confidentiality of the identity of the reporting person, of the person involved and of the person in any event mentioned in the report, as well as of the content of the report and of the relevant documentation.

c. The company has long had an organisational model pursuant to Legislative Decree 231/2001 and had therefore already introduced a procedure for reporting offences in accordance with the provisions of Law 179/2017. Legislative Decree 24/2023 confirms that the organisation and management models provide for internal reporting channels

d. Pursuant to Article 24 of Legislative Decree 24/2023, the Company is required to comply with the provisions from 15 July 2023

e. The Company is in the process of activating the internal channel for reporting by interested parties

f. The aforementioned Article 4 provides that the most representative national trade union representatives or organisations be consulted

That being stated, we hereby inform you of the following

1) The Company, as stated above, has defined the following internal channel(s) for the communication of offences falling under the aforementioned discipline, namely

.....

.....

(please indicate briefly the modalities also possibly with reference to a technical annex)

2) It should be noted that, also for reasons of greater security, the computerised channel (platform, PEC or dedicated email, etc.) should be preferred;
3) The company has also drawn up a specific procedure concerning the management of the i-channel that will be activated and the related notifications

4) The procedure provides for the respect of the confidentiality of the reporter, as established by the aforementioned provisions, as well as the identification of certain persons who may handle the information and carry out any investigations

5) The procedure provides for management and communication methods in compliance with the regulations

6) The company will also comply with the requirements set forth on the protection of personal data, as provided for in Articles 13 and 14 of Legislative Decree 24/2023

7) The company also undertakes to comply with the rules protecting the whistleblower and any other persons (Art. 17 et seq.), if the conditions exist

8) The company will provide employees and other persons with appropriate information on the reporting possibilities and the relevant channels, in particular by means of ..... (specify: website, e-mail, posters, etc.).

We look forward to your comments on the above by .....

Best regards.

for the Society

ANNEX 3

Report of misconduct form

DATA OF THE REPORTER	
NAME AND SURNAME	
QUALIFICATION	
ROLE	
OFFICE OF AFFILIATION	
TELEPHONE	
E-MAIL	
DATA/INFORMATION MISCONDUCT	
DESCRIPTION OF THE UNLAWFUL CONDUCT	
PERSON(S) WHO COMMITTED THE OFFENCE (Name, Surname, Title)	
ANY OTHER PERSONS INVOLVED	
DATE/PERIOD IN WHICH THE ACT OCCURRED	
PHYSICAL PLACE WHERE THE EVENT OCCURRED	
MANNER IN WHICH THE EVENT OCCURRED	
EVENTUAL FURTHER PERSONS WHO CAN REFER TO THE EVENT (Name, Surname, Title, Addresses)	
ANY OTHER USEFUL INFORMATION	
ANY ATTACHED DOCUMENTS	

ANNEX 4

Instructions for handling alerts

The reporting manager is obliged to process the information and reports received as follows:

It is considered that the person within the company or entity who can best take on the functions of managing reports is
Baker Tilly Rechtsanwaltsgesellschaft mbH
Nymphenburger Str. 3b
80335 München
Germany
Telephone: +49 89 55066-525
E-Mail: ombudsservice.swg@bakertilly.de

The managing entity shall be expressly trained on the contents of the legislation and the procedures required for its management and reporting.

The entity shall provide generalized information on the channel activated and on the relevant procedures.

Internal reports submitted to a person other than the one indicated shall be forwarded, within seven days of receipt, to the competent person, with simultaneous notification of transmission to the reporting person.

As part of the management of the internal reporting channel, the external person or entity entrusted with the management of the channel shall perform the following activities:

(a) issue the reporting person with an acknowledgement of receipt of the report within seven days from the date of receipt. This notice will preferably be sent to the address indicated by the reporting person in the report
(b) maintain contact with the person who issued the alert and may ask the latter for additional information if necessary
(c) diligently follow up the reports received
(d) acknowledge the report within three months from the date of the acknowledgement of receipt or, in the absence of such an acknowledgement, within three months from the expiry of the period of seven days from the submission of the report; acknowledgement must also be given if the report is not followed up or if the report is closed
(e) make available clear information on the channel, procedures and prerequisites for making internal reports, and on the channel, procedures and prerequisites for making external reports.

The information shall be displayed and made easily visible in the workplace, as well as accessible to persons who, although not frequenting the workplace, have a legal relationship relevant for the purposes of the legislation (e.g. e-mail communications).

Information on the channel and management is also included in a dedicated section of the aforementioned site.

In the event of malfunctions or anomalies in the systems, the operator shall promptly notify those responsible for intervention (IT or otherwise).

The operator will record the receipt of the report and keep it confidential, preferably omitting the names of the persons concerned.

In the event of a specific (oral or written) request by the reporting person, a face-to-face meeting should be arranged, within a reasonable period of time (generally within a maximum of five days, unless justified exceptions are made). It is preferable for the meeting to be held in premises outside the work context, and minutes will be taken of the meeting.

Upon receipt of the report, the operator shall:

- notify the reporting person of receipt of the report within 7 days of its receipt, unless the reporting person explicitly requests otherwise (fac simile A); the notice will be sent to the address indicated in the report

- liaise with the reporting person and request additions from the latter if necessary (fac simile B);

- diligently follow up the reports received

- carry out the necessary preliminary investigation to follow up the report, also by means of hearings and acquisition of documents;

- provide feedback to the reporting person within 3 months or, if there are justified and reasoned reasons, 6 months from the date of acknowledgement of receipt of the external report or, in the absence of such notice, from the expiry of 7 days from receipt (fac simile C)

- inform the reporting person of the final outcome of the report (similar D).

Compliance with the deadlines is important and must be scrupulously observed, since failure to do so allows the person concerned, as a general rule (except for violations relating to the organisational model pursuant to Legislative Decree 231/2001), to turn to the other reporting channels provided:

- external (reporting to ANAC
- public disclosure

Within the scope of the investigation, according to the information and training received, it may request any specific advice in the following manner, indicating that the investigation is covered by confidentiality and not revealing the names of the persons concerned.

…….. (specify: request to the manager, A.D. etc.)

The following elements should be taken into account when assessing the alert

- Subject: checking whether the report concerns a breach of the law [1]
- Content: assessment of whether the report is substantiated and provided with verifiable evidence [2]. The manager may use the form made available to the whistleblower as an outline for an initial assessment (see procedure - Annex 3)

[1] Specifically:
- administrative, accounting, civil or criminal offences Offences concerning violations of European legislation on public procurement, transport safety, environmental protection, radiation and nuclear safety, food and feed safety and animal health and welfare, public health, consumer protection, privacy and personal data protection, network and information system security; violations of competition and state aid legislationatti od omissioni che riguardano il marcato interno (ad es. concorrenza, aiuti di Stato)
- - unlawful conduct relevant under Legislative Decree No. 231/2001 ("predicate offenses") and violations of the related organization and management models

[2] Specifically, the required information is as follows:
- description of the offending conduct
- identity of the person making the report, indicating qualification/function/role performed
- clear and complete description of the facts being reported
- if known, the circumstances of time and place in which the facts were committed
- if known, the personal details or other elements that make it possible to identify the person who carried out the reported facts
- any additional persons who can report on the reported facts
- any additional documents that may confirm the substantiation of these facts
- any additional information that may provide useful feedback regarding the existence of the reported facts

- Work context: assessment of whether the reported events occurred in a work context [3]

The identity of the persons involved and of the persons mentioned in the report is protected until the conclusion of the proceedings initiated on account of the report, subject to the same guarantees provided for in favour of the person making the report. For the principle of minimisation, the data of persons not related to the report should be deleted.

If necessary, a supplement or additional information may be requested from the reporter. In this case, the above deadlines are interrupted until the requested information is provided or the deadline for providing it has expired (fac simile B cited above).

Reports from which the identity of the reporter cannot be established are considered anonymous.

If anonymous reports are received through internal channels, they shall in any case be considered as ordinary reports to be dealt with according to the above criteria, insofar as applicable, provided that the reports are substantiated and/or documented.

The person concerned may, or at his request, must be heard, possibly also by submitting written comments and documents. The person involved shall also benefit from the same confidentiality guarantees as the reporting person.

The identity of the whisteblower is protected both at the stage of acquiring the report and in any context following the report, except in cases where the identity must be revealed by law (e.g. criminal, tax or administrative investigations, inspections by control bodies, etc.).

If the charge is based, in whole or in part, on the report and knowledge of the identity of the reporter is indispensable for the defendant's defence, the report may only be used if the express consent of the reporter to the disclosure of his/her identity. In this case, information must be provided and the necessary consent requested and obtained (fac simile E).

It is forbidden to disclose data relating to the report, and in particular data concerning the identities of the persons concerned, except to expressly authorised persons or in cases provided for by law (e.g. legal proceedings).

The data must be processed in compliance with the security measures adopted and about which the manager has received adequate information.

The final outcome of the proceedings must be mandatorily communicated to the reporter (fac simile G)

Feedback must also be provided in the following cases:

- Lack of grounds [4]
- manifest groundlessness due to the absence of factual elements capable of justifying investigation

[3] The definition of work context is as follows:

- Work or professional activities, present or past, carried out within the framework of the relationships referred to in Article 3, paragraphs 3 or 4 of Decree 24/2023 [employees, collaborators, partners, shareholders, trainees, volunteers, freelancers, including during the probationary period and even if the relationship has ended], through which, regardless of the nature of such activities, a person acquires information about violations and within the scope of which he or she could risk retaliation in the event of a public report or disclosure or a complaint to the judicial or accounting authorities

[4] It should be noted, in particular, that the procedure does not apply, inter alia, to disputes or reports concerning individual employment relationships, or concerning relations with one's superiors (Art. 1 of Legislative Decree 24/2023), therefore, purely by way of example, it does not cover issues concerning the operation of employment relationships, e.g. non-payment, recognition of level, company organisation, working hours, disputes with superiors, etc.

- ascertained generic content of the report of offence such as not to allow comprehension of the facts, or report of offence accompanied by inappropriate or irrelevant documentation.

After the conclusion of the proceedings, the data collected may be retained for a maximum of five years.

Thereafter, they must be permanently deleted (see procedure for deletion of data).

Instructions to the alert manager

Templates and Facsimiles

Fac simile A

Notification to the person reporting the alert (within 7 days)

Fac simile B

Request for additional information from the reporting person

Fac simile C

Reply to person reporting the matter (within 3 months)

Fac simile D

Communication of final outcome to the reporting person

Fac simile E

Consent of reporting person

Fac simile A

Notification to the reporting person of receipt of the report (within 7 days)

Dear Sir/Madam

I hereby, as the manager of the reports of offences (Legislative Decree 24/2023) of the company/body _____

I hereby give notice

I have duly received and registered your report received on _____

I reserve the right to provide further feedback within the terms of the law.

The file is registered under no. _____ to which you may refer for further communications.

Best regards.

The manager

Fac simile B

Request for additional information from the reporting person

Dear Sir/Madam

Practice no. _____

Herewith, as manager of the reports of offences (Legislative Decree 24/2023) of the company/body _____

in relation to the file in question referred to in the notice of receipt of _____

having examined the file and assessed the lack of certain important elements for the purposes of assessing the report

I request

the following additional information: _____

the communication of the following documents _____

What is requested must be received in the same way as the report or at the following address _____ by _____

Once this deadline has passed without receipt of the requested documents, the file will be assessed on a de facto basis.

The deadlines for acknowledgement are suspended until notification of what has been requested or, in any case, until the deadline has expired.

Best regards.

The manager

Fac simile C

Reply to the reporting person (within 3 months)

Dear Sir/Madam

Practice no. _____

Herewith, as manager of the reports of offences (Legislative Decree 24/2023) of the company/body _____

in relation to the file in question referred to in the notice of receipt of _____

having assessed the file and the circumstances covered by the report

(if any) having also assessed the additions requested on _____ and communicated on _____

I hereby notify

that the following checks have been carried out _____

that the following measures have now been taken _____

We reserve the right to communicate the final outcome.

Best regards.

The operator

Fac simile D

Communication of final outcome to the reporting person

[can also replace fac simile C if final outcome is communicated within 3 months].

Dear Sir/Madam

Practice no. _____

Herewith, as manager of the reports of offences (Legislative Decree 24/2023) of the company/body _____

in relation to the file in question referred to in the notice of receipt of _____

having assessed the file and the circumstances covered by the report

(if any) having also assessed the additions requested on _____ and communicated on _____

I hereby notify

that the final outcome of the report was as follows

_____

Best regards.

The manager

Fac simile E

Consent of reporter

Dear Sir/Madam

Practice no. _____

Herewith, as manager of the reports of offences (Legislative Decree 24/2023) of the company/body

_____

in relation to the file in question referred to in the notice of receipt of _____

having examined the file and assessed the lack of certain important elements for the purposes of assessing the report

I inform

that it is necessary to know your identity within the framework of the disciplinary proceedings opened as a result of your report, for the following reasons:

_____

the data will be treated confidentially and will be communicated exclusively to

_____, with the obligation not to disclose or communicate them to unauthorized persons

Recalled the information on the processing of personal data already received by you at the time of the report

we request

your explicit consent to the above.

Best regards.

The manager

I, the undersigned _____

having taken note of the above and received the further information requested, in relation to the possibility of disclosure of my identity as indicated above

☐ I GIVE MY CONSENT ☐ I DENY CONSENT

_____, _____

Signature

ANNEX 5

Information to employees and third parties on reports

To employees/collaborators

To stakeholders

Subject: Legislative Decree 24/2023 - Reporting of offences (so-called 'Whistleblowing') - General information

In implementation of Directive (EU) 2019/1937, Legislative Decree No. 24 of 10 March 2023 was issued concerning 'the protection of persons who report breaches of Union law and laying down provisions concerning the protection of persons who report breaches of national laws'.

This legislation applies to public entities and private entities with more than 50 employees or even fewer employees, if a 231 organisational model has been adopted.

Our company/entity has adopted a specific procedure for dealing with whistleblowing, as the conditions are met.

A person who reports wrongdoing within the company/entity is commonly referred to as a "whistleblower".

This term refers not only to the employee or collaborator of an entity or a company but also to other persons (e.g. employee of a supplier, shareholders, partners, etc.), who report violations of national or European Union regulations that harm the public interest or the integrity of the public administration or the private entity, of which they have become aware in a work context.

(for those who have adopted the 231 organisational model) In addition, for those who have adopted an organisational model pursuant to Legislative Decree 231/2001, the reports may also concern the so-called 'predicate offences' and the model itself.

Whistleblowing, in the intentions of the legislator, is a manifestation of civic sense through which the whistleblower contributes to the emergence and prevention of risks and situations prejudicial to the organisation to which he or she belongs.

Disclosures or whistleblowings can be of various kinds: violation of a law or regulation, threat to a public interest as in the case of corruption and fraud, serious and specific situations of danger to public health and safety, etc.

Reporting is therefore an important preventive tool.

Within the framework of the prepared procedure, the company/entity has defined

- The 'channel' through which reports are made (so-called 'internal channel')
- The entities authorised to handle alerts and define the procedure
- The procedure following the report
- Communications to the reporter
- Safeguards for the reporter and other subjects
- Security measures
- Privacy procedures and disclosures

Some useful pointers are given below.

Who can report wrongdoing

Employees, self-employed workers, holders of a collaboration relationship providing goods or services or carrying out works in favour of the company/entity, freelancers and consultants, volunteers and trainees, whether paid or unpaid, shareholders, partners and persons with administrative, management, control, supervisory or representative functions.

Persons whose employment relationship has ended may also report if the report concerns incidents that occurred during the course of the relationship and candidates for employment who have acquired the information on violations during the selection process or at other stages of pre-contract negotiations.

What is the subject of alerts

- Administrative, accounting, civil or criminal offences
- Offences concerning breaches of European legislation on public procurement, transport safety, environmental protection, radiation protection and nuclear safety, food and feed safety and animal health and welfare, public health, consumer protection, protection of privacy and personal data protection, network and information system security; breaches of competition law and state aid
- Acts or omissions affecting the internal market (e.g. competition, state aid)
- (in the case of model 231) Illegal conduct relevant under Legislative Decree no. 231/2001 ("predicate offences") and violations of the relevant organisation and management models.

What should not be reported

- Reports must relate to facts occurring in the 'employment context'. This term refers to work or professional activities, present or past, carried out in the context of the relationships referred to in Article 3(3) or (4) of Legislative Decree 24/2023 [employees, collaborators, partners, shareholders, trainees, volunteers, freelancers, even during the probationary period and even if the relationship has ended], through which, regardless of the nature of such activities, a person acquires information about violations and in the context of which he/she could risk retaliation in the event of a report or public disclosure or a complaint to the judicial or accounting authorities. Reports that concern personal or family relationships or other relationships that are not work-related are therefore not included.
- The procedure also does not apply to complaints or reports concerning individual employment relationships, or concerning relations with one's superiors (Article 1 of Legislative Decree 24/2023).
- Therefore, purely by way of example, it does not cover issues concerning the operation of labour relations, e.g. non-payment, recognition of level, company organisation, working hours, etc. (they may instead concern discriminatory behaviour or behaviour that does not respect gender equality).

The content of the reports

Reports must be detailed and documented as far as possible, in order to enable the person handling them to have the necessary information to proceed with any investigations.

For example, the description of the fact being reported must be clear and complete, the reference period must be specified, the author(s) of the facts must be identifiable, and any documents supporting what has been reported must be attached where possible.

In order to provide help, an outline has been prepared, which may constitute an outline for making the report

Anonymous reports

Anonymous reports shall be treated as ordinary reports to be dealt with according to the criteria laid down in this procedure, insofar as applicable, but the reports must be substantiated and documented.

The 'internal' reporting channel

The company/entity has adopted the following reporting methods

In particular, in the case of a paper report or in the case of a request for an oral interview, the communication should be made in a sealed (anonymous) envelope with the following wording on the envelope: "whistleblowing" or "whistleblowing".
The report may be sent by post or placed in the box provided for this purpose.

Managing entity

The company/entity has appointed certain individuals, expressly authorized, trained and bound to confidentiality, to handle the reports

Upon receipt of the report, the reporter will be notified (at the address provided) and feedback on the report will be provided within three months. The final outcome of the investigation, if subsequent, will also be communicated.

The managers identified for the processing of reports are as follows:
.....
.....
(also only indication of the function and not the person)

Where reports concern managers, the report should be addressed to .....

Translated with DeepL.com (free version)

Protections for the reporter

The identity of the whisteblower is protected both at the stage of acquiring the report and in any context following the report, except in cases where the identity must be detected by law (e.g., criminal, tax or administrative investigations, inspections by supervisory bodies, etc.).
(*possible*) ***LINK TO PRIVACY POLICY***

If the dispute is based, in whole or in part, on the report and knowledge of the identity of the reporter is essential for the defense of the accused, the report may be used only if the reporter's express consent to the disclosure of his or her identity is present. In such a case, the necessary consent will be sought and acquired.
The identity of the persons involved and the persons mentioned in the report shall be protected until the conclusion of the proceedings initiated on account of the report in accordance with the same guarantees provided in favor of the reporter. For the principle of minimization, data of persons not related to the report will be deleted.
Towards the reporting party (as well as other parties), no form of retaliation or discriminatory measure is allowed or tolerated.
The protective measures consist of the

- prohibition of retaliatory acts, which include, but are not limited to, dismissal, demotion, transfer of location and any other action that entails negative effects on employment contracts,

as well as a range of other "punitive" conduct, such as requiring submission to medical or psychiatric examinations,

- prohibition of discriminatory actions from which economic or financial prejudice, including in terms of loss of income or opportunity, results.

Protection measures do not apply when the criminal liability of the reporting person for the crimes of defamation or slander, or his civil liability, for the same title, in cases of willful misconduct or gross negligence, is established, even by a judgment of first instance. In such cases, a disciplinary sanction shall also be imposed.

External reporting and public disclosure

External reporting means the written or oral communication of information about violations submitted through the reporting channel activated by the National Anticorruption Authority (ANAC).

The reporter may use the ANAC channel if one of the following conditions is met:

- there is no provision for mandatory activation of the internal reporting channel within the work environment of the reporter, or this channel, even if mandatory, is not active or, even if activated, does not comply with the provisions of Legislative Decree No. 24 of 2023
- the reporter has already made an internal report and it has not been followed up
- the reporter has well-founded reasons to believe that, if he or she made an internal report, it would not be effectively followed up or could result in the risk of retaliation; - the reporter has well-founded reasons to believe that the violation may constitute an imminent or obvious danger to the public interest.

Disclosing reports publicly, on the other hand, means placing information about violations in the public domain through print or electronic media or otherwise through means of dissemination that can reach a large number of people.

A reporter who makes a public disclosure benefits from the protection regime governed by Decree No. 24 of 2023 if, at the time of the public disclosure, one of the following conditions is met:

- the reporting person has previously made an internal and external report, or has made an external report directly, under the conditions and in the manner prescribed by the regulations, and the report has not been followed up or acknowledged within the terms of the law
- the reporting person has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest
- the reporting person has well-founded reason to believe that the external report may pose a risk of retaliation or may not be effectively followed up due to the specific circumstances of the concrete case, such as those where evidence may be concealed or destroyed or where there is a well-founded fear that the person who received the report may be colluding with or involved in the perpetrator of the violation.

Note: It should be noted that external and, especially, public reporting should be done only when there are specific documented and provable conditions, as they may involve the image of the company/entity, otherwise the internal channel should be preferred.

More Information

More details or information on the procedure and the reports in question can be obtained at ..... or by sending an email to .....

ANNEX 6
Authorization to process data

Dear Mr./Mr. Ms.

…….

Subject: permission to process personal data

Given E.U. Regulation 2016/679 and implementing regulations, we clarify the following.

Whereas

- That our organization has adopted a system of reporting wrongdoing as required by Legislative Decree 24/2023 and in particular has activated its internal channel in the following manner:

……
……
……

(describe mode of reporting through internal channel)

- that pursuant to Article 10 of the aforementioned Legislative Decree 24/2023, the Data Controller has examined the repercussions on the processing of personal data, adopting appropriate security measures, in compliance with data minimization
- That you have been identified for the purpose of handling the reports
- that, in this regard, you have received appropriate information as well as specific training on the content of the law and on how to manage data relating to reports of wrongdoing, particularly with reference to the protection of the confidentiality of the reporter and other interested parties
- that it is necessary, pursuant to EU Regulation 2016/679 a specific authorization for the processing of personal data, in relation to what is reported through the internal channel(s) adopted by the entity

All of the above we confirm the following:

1) You are authorized to process personal data used in the context of the entrusted services and specifically in the context of the management of reports, in any way received, in relation to the procedure adopted for the reporting of offenses under Legislative Decree 24/2023.

Therefore, in the performance of your activities may perform the processing of personal data to which it has access and inherent to these activities.

Given the type of service you provide, the processing will in principle take place with mechanized systems, not excluding, however, paper-based systems, and may include all the operations referred to in point 2 of Article 4 of the aforementioned Regulations.

2) Access to the data will have to be implemented in such a way as to avoid unauthorized access or dissemination of data, performing the operations strictly necessary for your activity.
3) We specify that for access to the personal data and archives to which your specific activity is entrusted, you will have to use an identification code assigned to you confidentially as well as a keyword prepared by you composed of at least eight characters. This keyword will have to be replaced by you every time you are expressly requested to do so by the system and in any case with a constant periodicity.
4) Please remember that the identification code, if used, as well as your keyword, are strictly personal and cannot be used by others. Violation may constitute a criminal offense.
5) Authorization systems, such as keyword or the like, other than those authorized for technical management purposes only, will be automatically deactivated if no longer used

6) We remind you that for each intervention you will have to take care that the computer tool used does not remain unattended or accessible to others in your absence; in particular in case of absence you will have to make sure that the workstation is protected by checking the relevant protections.
7) The use of removable media for the storage of the data mentioned above is prohibited.
8) Generally for the type of activity he will have to deal with common data. However, it is not excluded that it must also sporadically carry out processing operations in relation to special data (Art. 9 EU Regulation 2016/679) or judicial data, if present in the reports.
9) In case of data processing with non-automated (paper) systems, you will have access only to the data whose knowledge is necessary for the performance of the activity entrusted to you.
10) Also in the case of data processing with non-automated (paper) systems, the acts and documents concerning the data in question will have to be kept by you in such a way as to prevent intrusion or unauthorized access, recalling again that the protection of the secrecy of the identity of the reporter or other subjects is pre-eminent in the case.
    These precautions must also be observed in the case of reproduction on paper documents or similar of information relating to the processing of sensitive data
11) Insofar as it is the subject of separate specific directions, we also remind you that corporate requirements regarding data breach or loss (data breach) must be scrupulously observed

Best regards

_____, _____

The Data Holder

As receipt:

_____, _____

_____

ANNEX 6 bis

DATA PROCESSING AUTHORIZATION (ODV)

Dear Mr./Mr. Ms.

…….

Supervisory personnel

Subject: personal data processing authorization - OdV

Given E.U. Regulation 2016/679 and implementing regulations, we clarify the following.

Whereas

- that our organization has adopted a system of reporting wrongdoing as required by Legislative Decree 24/2023 and in particular has activated its internal channel in the following manner:
  .....
  .....
  .....

(describe mode of reporting through internal channel)

- that pursuant to Article 10 of the aforementioned Legislative Decree 24/2023, the Data Controller has examined the repercussions on the processing of personal data, adopting appropriate security measures, in compliance with data minimization
- that the Supervisory Body (or Chairman of the Supervisory Body) ex Dlgs. 231/2001 has been identified as the manager for the purposes of the reports received
- that this Body has been considered by the Guarantor of Personal Data Protection (see opinion dated May 12, 2020 prot. no. 17347) an organ of the companies or entities and as such should be authorized to process data, if necessary
- that in this regard he/she has received appropriate information as well as specific training on the content of the law and on how to manage data relating to reports of wrongdoing, in particular with reference to the protection of the confidentiality of the reporter and other interested parties
- that in any case on the basis of experience and professional training is capable of carrying out the assigned task
- that it is necessary, pursuant to EU Regulation 2016/679 a specific authorization to the processing of personal data, in relation to what is reported through the internal channel(s) adopted by the entity

All of the above we confirm the following:

1. You are authorized to process personal data used within the scope of the entrusted services and specifically within the scope of the management of reports, in any way received, in relation to the procedure adopted for the reporting of offenses pursuant to Legislative Decree 24/2023.
2. Therefore, in the performance of its activities may perform the processing of personal data to which it has access and inherent to these activities.
3. Given the type of service provided by you, the processing will in principle take place with mechanized systems, not excluding, however, paper-based systems, and may include all the operations referred to in point 2 of art. 4 of the aforementioned Regulations.
4. Access to data must be implemented in such a way as to avoid unauthorized access or dissemination of data, performing the operations strictly necessary for your activity.
5. We specify that for access to personal data and archives to which your specific activity is entrusted, you will have to use an identification code assigned to you confidentially as well as a keyword prepared by you composed of at least eight characters. This keyword will have to be sostituita ogni volta che verrà fatta espressa richiesta in tal senso dal sistema e comunque con una costante periodicità.

6. Please remember that the identification code, if used, as well as your keyword, are strictly personal and cannot be used by others. Violation may constitute a criminal offense.
7. Authorization systems, such as password or the like, other than those authorized for technical management purposes only, will be automatically deactivated if no longer used
8. We remind you that for each intervention you will have to take care that the computer tool used does not remain unattended or accessible to others in your absence; in particular in case of absence you will have to make sure that the workstation is protected by checking the relevant protections.
9. It is forbidden to use removable media for storing the cited data.
10. Generally for the type of activity he will have to deal with common data. However, it is not excluded that it will also have to sporadically carry out processing operations in relation to special data (Art. 9 EU Regulation 2016/679) or judicial data, if present in the reports.
11. In case of data processing with non-automated (paper) systems, you will have access only to the data whose knowledge is necessary for the performance of the activity entrusted to you.
12. Also in the case of data processing with non-automated (paper) systems, the acts and documents concerning such data will have to be kept by you in such a way as to prevent intrusion or unauthorized access, recalling again that the protection of the secrecy of the identity of the reporter or other subjects is preeminent in the case.
13. These precautions should also be observed in the case of reproduction on paper documents or similar of information related to the processing of sensitive data.
14. To the extent that this is the subject of separate specific guidance, we also remind you that corporate requirements regarding data breach or loss (data breach) must be scrupulously observed

Best Regards
_____, _____

Treatment owner

Per receipt
_____, _____

_____

ANNEX 7

Privacy Policy

E.U. Regulation 2016/679 and Legislative Decree 196/03 ("Personal Data Protection Code")
Unlawful reporting (Legislative Decree 24/2023)
Disclosure

1. Foreword

We inform you that pursuant to EU Regulation 2016/679 and Legislative Decree 196/03 ("Code for the Protection of Personal Data") and subsequent amendments, that the personal data provided by you, or acquired, as part of the procedure for reporting wrongdoing (so-called whistleblowing") referred to in the special procedure defined by the company/entity will be processed in compliance with the provisions of the law by the parties involved in the aforementioned procedure, subject to the obligation of confidentiality and protection as well as the requirements of the legislation (Legislative Decree 24/2023).

2. Data processed and purposes

The processing of data, generally common, is therefore aimed exclusively at the fulfillment of legal obligations under the procedure for reporting offenses, as analytically established by law as well as by the procedure defined by the company/entity [if adopted model 231 add: as an integral part of the model ex Dlgs. 231/2001].

3. Legal basis of processing

The legal basis of the processing is constituted by the aforementioned legislation (Dlgs. 24/2023 and succ. modif.) The legal basis is also constituted by the express consent of the person concerned for the disclosure of the identity of the person concerned and in particular in cases where the disciplinary charge against the accused is based, in whole or in part, on the report and the knowledge of the identity of the reporter is indispensable for the defense of the accused.

In such cases, the whistleblower will be asked to give consent or not.

4. Recipients of the data

The data are not subject to disclosure to third parties except as part of the procedure or in case of a request by investigative bodies.

5. Period of data retention.

The data will be kept for the period necessary for the completion of the procedure and the consequent fulfillments, except for the requirements of justice or discipline, and in any case for a maximum period of five years.

6. Mandatory

The provision of data necessarily results from the report made.

7. Type of processing

The data will be included in our archives, in particular in the database "Reporting of offences " and their processing, which may be carried out through automated and/or paper-based means, will include all the operations or set of operations provided for in Art. Art. 4 no. 2 of the Regulations and necessary for the processing in question, namely: collection, recording, organization, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, comparison or interconnection, restriction, deletion or destruction.

The Data Controller has also ensured that the security measures taken are correct.

8. Authorized parties

The Data Controller has taken steps to identify and train one or more persons expressly authorized to process the data, who are also bound by the special obligations under Legislative Decree 24/2023 regarding confidentiality.

9. Data controller

Data controller is .....

10. Data processor [if prerequisites are met].

In connection with the outsourcing to external parties of certain activities to be performed on behalf of the Data Controller (such as managing the receipt of reports), the Data Controller has appointed a Data Processor

11. external processing by defining its activity and acquiring information on security measures. More information available with a request at ..... or at .....

12. Data protection officer [if any, if appointed].

The company/entity has appointed pursuant to Articles 37 et seq. of the EU Regulation 2016/679 the Data Protection Officer (DPO), also definable as "Data Protection Officer" (DPO), whose contact details can be found on the website ..... or can be requested from .....

13. Transfer of data

Data, in compliance with the confidentiality set forth in Legislative Decree 24/2023, will not be transferred or otherwise stored outside the E.U.

14. Rights of the data subject

According to Art. 2 undecies of Legislative Decree 196/2003 recalled by Art. 13 of Legislative Decree 24/2003, the right of access to personal data, the right to rectify them, the right to obtain their deletion 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 or the right to complain to the Guarantor may be restricted or not be exercised if the exercise of these rights may result in actual and concrete harm to the person who reported the wrongdoing.

According to the ANAC Guidelines This could result in actual and concrete prejudice to the protection of the confidentiality of the identity of the reporting person from the exercise of these rights, and therefore these powers are precluded in the processing of data related to the procedure for reporting wrongdoing.

Treatment Owner

ANNEX 8
DPIA

Per l'utilizzo del software gratuito messo a disposizione dal Garante

https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

Per ulteriori informazioni sulla valutazione di impatto:

https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia-

ANNEX 9

Compliance checklist Data controller

COMPLIANCE CHECKLIST

Name of data processor	

Reference is made to the definitions in the Deed of Appointment of Data Processor received.

Section A - Data and processing methods.

	Requirement	Response
1	Are processed : i. types of personal data other than those listed in the Deed of Appointment or data subjects other than those listed therein? ii. personal data for purposes other than those listed in the Deed of Appointment? iii. personal data in locations other than those listed in the Deed of Appointment?	Yes☐ No ☐

Section B – Organizational Measures

	Requirement	Response
1	Have all Appointees received appropriate letters of appointment along with the instructions contained in this Appointment Deed?	Yes ☐ No ☐ N/A ☐
2	Do all Appointees attend periodic training courses focused on their obligations under the Privacy Regulations?	Yes ☐ No ☐ N/A ☐
3	Is there an updated register of processing activities regarding Personal Data?	Yes ☐ No ☐ N/A ☐
4	Has a Data Protection Officer been appointed?	Yes ☐ No ☐ N/A ☐
5	Has written authorization from the Data Controller been obtained before proceeding with the appointment of Sub-Processors?	Yes ☐ No ☐ N/A ☐
6	Has the adequacy of the technical and organizational capabilities of each Sub-Responsible person been verified (and is it verified at least annually) through the completion of this Compliance Checklist, which each Sub-Responsible person is required to complete both at the time of their appointment and at least annually?	Yes ☐ No ☐ N/A ☐
7	Each Sub-Responsible Officer has been appointed on the basis of an agreement, the content of which is substantially in line with the content of this Deed of Appointment.	Yes ☐ No ☐ N/A ☐
8	Has a policy regarding the handling of Personal Data been adopted within the security policy?	Yes ☐ No ☐
9	Has a specific policy regarding passwords been planned and documented?	Yes ☐ No ☐

Section C – Technical Measures

	Requirement	Response
1	Do you have appropriate technical and organizational measures in place to prevent unlawful processing of the Controller's Personal Data in violation of the obligations under this Deed of Appointment?	Yes ☐ No ☐
2	Is there a procedure in place to notify a possible breach of Personal Data by the Appointees?	Yes ☐ No ☐
3	Do you have technical and organizational measures in place to enable the deletion, rectification, updating, restriction of processing and portability of Personal Data at the request of the Data Controller and/or upon termination of the Contract?	Yes ☐ No ☐
4	Do you have technical measures in place to enable the return of Personal Data to the Data Controller upon its request and/or upon termination of the Contract?	Yes ☐ No ☐
5	Are Personal Data Trustees' accesses protected by technical measures, including IDs, passwords, antivirus and firewalls, intrusion detection systems, logging and monitoring, and network flow encryption?	Yes ☐ No ☐
6	Do you have a two-factor authentication system, which is advisable with regard to access to systems that process sensitive data?	Yes ☐ No ☐ N/A ☐
7	Do you have technical measures in place that allow access to Personal Data only to those Trustees who need access for reasons related to the performance of the Contract?	Yes ☐ No ☐
8	Do you have technical measures in place to ensure the ongoing confidentiality, integrity, availability and resilience of data processing systems and services?	Yes ☐ No ☐
9	Do you have technical measures in place to ensure that the workstations, both fixed and mobile, used by your staff and the staff of your Sub-recipients for the provision of the services are adequate to prevent any breach or defect inherent in security?	Yes ☐ No ☐
10	Do you have additional technical procedures that are regularly performed in order to verify the adequacy of security measures to protect access to Personal Data (e.g., application lifecycle security procedure, change management procedure, vulnerability management procedure, data backup and recovery procedure, business continuity procedures, audit procedures)?	Yes ☐ No ☐
11	Have you introduced specific measures to protect confidentiality ex Dlgs. 24/2023?	Yes ☐ No ☐

Signature of the legal representative of the -Responsible

Date: _____

Role : _____

Name: _____

Signature: _____

ANNEX 10

Fac simile Treatment Register (simplified)

TREATMENT LOG SHEET n. ____	Established on _____	Last updated on _____
OWNER:		
DATA PROTECTION OFFICER:		

TYPE OF PROCESSING	PURPOSE AND LEGAL BASIS FOR PROCESSING	CATEGORIES OF DATA SUBJECTS	CATEGORIES OF PERSONAL DATA	CATEGORIES OF RECIPIENTS	[TRASFER OF DATA TO THIRD COUNTRIES OR ORGANIZATIONS INTERNATIONALS]	EXPECTED DELETION DEADLINES	TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES
Management of reports of wrongdoing (whistleblowing) ex Dlgs. 24/2023	a) Fulfilment of legal obligations under the procedure for reporting wrongdoing, as analytically established by law as well as by the procedure defined by the company/ as an integral part of the model ex Dlgs. 231/2001 b) Disclosure of identity of the interested party c) Case in which the disciplinary charge against the accused is based, in whole or in part, on the report and knowledge of the identity of the reporter is essential for the defense of the accused Legal basis Legal obligation Consent (lett. b and c)	Employees (including terminated), Collaborators Directors Auditors Third parties Trainees	Municipalities Particulars Judiciary	Expressly authorized persons	NO	Period necessary for the completion of the procedure and the consequent fulfillments, except for judicial or disciplinary requirements, and in any case for a maximum period of five years from the termination of treatment	V. list

Model conforms to the guidance of the Guarantor (https://www.garanteprivacy.it/en/home/faq/registro-delle-attivita-di-trattamento

ANNEX 11

Fac simile communication to the SB

From _____

To the Supervisory Board ex Dlgs. 231/2001

Subject: Legislative Decree 24/2023

We hereby inform you, for any appropriate evaluation by this Body, that within the internal channel adopted by the company/entity pursuant to Art. 4 of Legislative Decree 24/2023, a report has been received concerning the following violation of the organizational model and/or predicate offenses:

_____

_____

As is known, the identity of the reporter and other persons involved is protected under the aforementioned provisions and the same benefit from specific forms of protection. Therefore, no further details are provided, which could lead back to such identity.

_____, there _____

ANNEX 12

Diagram using signaling channels