SAES Group

Whistleblowing policy

Updates	Date	Approved
Adoption	19/07/2018	Board of Directors
First revision	18/06/2020	Board of Directors
Second revision	11/11/2022	Chairman of the Board of Directors
Third revision	13/07/2023	Board of Directors

Contents

1. Objective

The purpose of this document is to remove the factors that may hinder or discourage the use of ***whistleblowing***, introduced into Italian law by Law No. 179 of 30 November 2017.

Following the issuance of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, the legislation on whistleblowing was standardised and some controls were strengthened. The aforementioned Directive was introduced into Italian law by Legislative Decree no. 24 of 10/03/2023 (hereinafter also the "***Regulation***"), which repealed the previous national regulations (including Law no. 179/2017) and included in a single regulatory text the regime for the protection of subjects who report unlawful conduct that violates European and national provisions, based on well-founded reasons and detrimental to the public interest or the integrity of the entity to which they belong.

The regulations contain provisions for the protection of those who report crimes or irregularities of which they become aware in the context of a public or private employment relationship. From this perspective, the objective pursued by this procedure is to provide the whistleblower with clear operational instructions on the subject, content, recipients and methods of transmission of the reports ("***Reports***" or, in the singular, "***Report***"), as well as about the forms of protection offered to him/her, to remove doubts and uncertainties about the procedure to be followed and any fears of retaliation or discrimination.

The objective of the policy and of the whistleblowing system is to ensure protection for those who report non-compliance with laws or regulations, policies, rules or company procedures (in particular, also with reference to the scope of the predicate offences and the risk areas defined in the Organisational Model pursuant to Italian Legislative Decree No. 231/01), as indicated in more detail below in this document. The objective of the tool is to prevent and detect the occurrence of irregularities within the organisation, in order to remedy and correct them, but also to involve all stakeholders, in general, in activities to combat non-compliance, through active and responsible participation.

SAES Getters SpA ("***SAES***" or the "***Company***") provides a specifically dedicated internet platform with free access by the parties entitled to do so by the Regulations (as listed below) as a channel for the reporting of acts or omissions by anyone within the SAES Group, in relations with the individual companies of the SAES Group or on their behalf, which constitute or may constitute a violation, or inducement to violate laws and regulations, principles set out in the Code of Ethics, principles of internal control, company policies, rules and procedures and/or may directly or indirectly result in economic, financial or image-related damage for the companies of the SAES Group (as better specified below).

2. Objective scope of application

Pursuant to art. 2 of Legislative Decree No. 24 of 10/03/2023, the following violations may be reported:

- administrative, accounting, civil or criminal offences;
- significant unlawful conduct pursuant to Legislative Decree 231/2001[1] or the OMM;
- offences falling within the scope of EU or national acts[2];
- acts or omissions that harm the EU's financial interests;
- acts or omissions concerning the internal market (Article 26(2) of the TFEU);

[1] Reports of offences pursuant to Italian Legislative Decree no. 231/2001 can only be carried out through internal channels.

[2] including offences relating to the protection of personal data and the security of networks and IT systems.

- acts and conduct that nullify the object and purpose of the provisions referred to in the EU acts in the sectors indicated in nos. 3-4-5.

Pursuant to art. 1(2) of Legislative Decree No. 23/2023, whistleblowing does not apply:

a) to disputes, claims or requests related to a personal interest of the whistleblower or person who lodges a complaint with the judicial or accounting authority that relate exclusively to their individual employment or public employment relationships, or inherent to their relationships of work or public employment with hierarchically superior figures;
b) to reports of violations where already mandatorily regulated by the European Union or national acts indicated in Part II of the Annex to this decree or by national ones that constitute an implementation of the European Union acts indicated in Part II of the Annex to Directive (EU) 2019/1937, although not indicated in Part II of the Annex to this decree;
c) to reports of violations relating to national security, as well as contracts relating to aspects of defence or national security, unless these aspects fall under the relevant secondary legislation of the European Union.

Communications relating to commercial activities (e.g. complaints for invoicing, warranties, products, etc.) must be channelled through the customer service tools envisaged for the purpose.

The data subject shall exercise his/her rights, for privacy purposes, by e-mail to privacy@saes-group.com. This is without prejudice to any legal obligations, in particular with regard to the obligation to report to the Judicial Authority or to the Supervisory Authorities or to the Privacy Guarantor regarding the processing of personal data and protection of privacy envisaged by the law.

The Policy does not modify in any way, for companies within the SAES Group under Italian law, the methods of reporting to the Supervisory Bodies, where established, and their supervisory powers for the matters within their remit, in accordance with the provisions of current legislation and the Organisational Models adopted pursuant to Legislative Decree 231/2001 by the individual companies.

3. Subjective scope of application

Pursuant to art. 3 of Legislative Decree no. 24 of 10/03/2023, the subjects entitled to make Reports are all employees of the SAES Group, as well as freelancers, consultants, , suppliers and subcontractors (including employees and collaborators of the same), volunteers and trainees (paid and unpaid), shareholders and persons with administrative, management, control, supervisory or representative functions who work for the SAES Group, former employees, former collaborators or persons who no longer hold one of the positions indicated above, persons undergoing probation, selection, or whose legal relationship has not yet begun, as well as any other person entitled to submit reports under the Regulations.

The protection regulations envisaged for the aforementioned Whistleblowers are also extended to the following parties:

- facilitators[3];

[3] "Facilitator" means a natural person who assists the Whistleblower in the Reporting process, operating within the same working context and whose assistance must be kept confidential.

- persons in the same working context as the Whistleblower, the person who filed a complaint with the judicial or accounting authority or who made a public disclosure and who are linked to said person by a stable emotional bond or kinship up to the fourth degree;
- the work colleagues of the Whistleblower or the person who has filed a complaint with the judicial or accounting authority or made a public disclosure, who work in the same working context as him/her and who have a habitual and current relationship with said person;
- if applicable, entities owned by the Whistleblower or by the person who has lodged a complaint with the judicial or accounting authority or who has made a public disclosure or for which the same persons work, as well as entities that operate in the same working context as the aforementioned persons;
- anonymous Whistleblowers, if subsequently identified and subject to retaliation.

4. Internal Reporting Channels

4.1 On-line platform for Reports

Reports can be submitted by accessing the homepage of the company website (in the dedicated section) or by clicking directly on: *https://segnalazioni.saesgetters.com*.

It should be noted that access to the Whistleblowing platform through the SAES website is subject to the 'no-log' policy: this means that, even if access to the Whistleblowing platform is carried out from a computer connected to the company network, it would not, in any case, be tracked by the company information systems, to ensure further protection of the whistleblower.

The platform is external to the SAES website and network and uses Globaleaks, open-source and free software created to allow the launch of secure and anonymous whistleblowing initiatives. The software is developed by the Hermes Center for Transparency and Digital Human Rights.

The Platform allows the whistleblower to send reports in written form (by completing a questionnaire) or, at the request of the whistleblower, in oral form (by means of a personal meeting with the Recipient who will be fixed within a reasonable time).

4.2 Dedicated e-mail address

Reports can also be made by e-mail to the e-mail address *signalazioni@saes-group.com*.

Reports received in the mail box are accepted provided that the fact reported is described in detail and contains accurate information, including but not limited to: i) description of the event, ii) time and place, iii) personal details of whoever has committed the act, iv) any witnesses and relevant documentation.

Reports received via the e-mail address *signalazioni@saes-group.com* are entered in the whistleblowing portal by the Recipient in order to keep track of them.

5. Additional Reporting channels

Pursuant to the Regulations, Reports may be sent through additional channels: the External Reporting Channel and Public Disclosure.

5.1. External Reporting Channel

The External Reporting Channel is activated by the National Anti-Corruption Authority (ANAC), which ensures, including through the use of encryption tools, the confidentiality of the identity of the Whistleblower, the person involved and the person mentioned in the Report, as well as the content of the Report and related documentation.
The same confidentiality is also guaranteed when the Report is made through different channels or is received by personnel other than those responsible for processing the Reports, to whom it is in any case sent without delay.

Conditions for making external Reports

The Whistleblower may make an external Report if, at the time of its submission, one of the following conditions is met:

- the mandatory activation of the internal reporting channel is not envisaged as part of the work context or, even if mandatory, is not active or, even if activated, does not comply with the provisions of art. 4 of Legislative Decree No. 24 of 10/03/2023;
- the Whistleblower has already made an internal Report pursuant to art. 4 of Legislative Decree no. 24 of 10/03/2023 and this was not followed up;
- the Whistleblower has reasonable grounds to believe that, if s/he makes an internal Report, it will not be effectively followed up or that said Report may lead to a risk of retaliation;
- the Whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.

Methods for making external Reports

External Reports are made in writing via the IT platform or orally through telephone lines or voice messaging systems[4] or, at the Whistleblower's request, by means of a direct meeting [5]set within a reasonable time.

An external Report submitted to a party other than the ANAC is sent to the latter within 7 (seven) days from the date of its receipt, with simultaneous notice of the sending issued to the Whistleblower.

For more details on the External Reporting Channel, please refer to the ANAC website.

5.2 Public Disclosure

A Whistleblower who makes a public disclosure shall benefit from the protection envisaged by Italian Legislative Decree 24/2023 if, at the time of public disclosure, one of the following conditions is met:

a) the Whistleblower has previously made an internal and external Report or has made an external report directly and no response has been given within the prescribed terms;
b) the Whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest;

[4] If a recorded voice messaging system is used, the Report, subject to the Whistleblower's consent, is documented by the Recipient by recording on a device suitable for storage and listening, or by means of a full transcription. In the latter case, the Whistleblower may verify, rectify or confirm the content of the transcript by signing it.

[5]When the Report is made during a direct meeting, it is documented by the Recipient by recording it on a device suitable for storage and listening, or by means of a report. In the latter case, the Whistleblower may verify, rectify or confirm the minutes of the meeting by signing it

c) the Whistleblower has reasonable grounds to believe that the external report may involve a risk of retaliation or may not have an effective follow-up due to the specific circumstances of the case in question.

6. Content of Reports

Reports must be made in good faith; must be substantiated with precise information, in order to be verified and managed without the need to involve the Whistleblower and corroborated by elements that are not clearly baseless. More specifically, the Report must: a) contain a clear and complete description of the event; b) define the circumstances of time and place where the event occurred; c) indicate the personal details (where possible) of the person who carried out the facts; d) indicate (where possible) the parties witnessing the event; e) refer to relevant documentation and how the events were revealed.

With reference to the Whistleblowing portal, the platform provides a guided path for the Whistleblower, through a series of questions, open and closed, some mandatory, others optional, which concern facts, time context, economic dimensions, details of the Whistleblower (optional), additional supporting elements, with the aim of obtaining, right from the start, a screening of irresponsible or insignificant Reports.

It is not necessary to provide the personal details of the Whistleblower: the Report may also be made in a totally anonymous form.

The Whistleblower always has the option of requesting, both through the dedicated e-mail address and through the Platform, an in-person meeting with the subject receiving the Report (defined below).

7. Sending of Reports

With reference to the Whistleblowing portal, at the end of the Report, the Whistleblower is provided with a code through which s/he can then access his/her Report again and monitor its progress. In this way, it is possible to establish a form of direct dialogue with the Whistleblower, also in a completely anonymous form, through which it is possible to request, if necessary, additional detail or elements in support of the Report itself. A copy of the Report is not sent to the Whistleblower, who is therefore invited to take note of the identification code of the Report in order to be able to re-access it.

A Report sent to a party other than the Recipient (e.g. to a company Function not responsible for managing the Reports) must be sent within 7 (seven) days of receipt to the Recipient, who simultaneously informs the Whistleblower.

8. Management of Reports

8.1 Reports sent via the Whistleblowing portal and/or by e-mail to the address *certificazioni@saes-group.com* can only be viewed by persons from the Legal & Compliance Function of SAES, duly trained and appointed to process the personal data contained in the Reports and subject to confidentiality obligations (referred to hereinafter, individually or jointly, as the "***Recipients***"[6]).

Within 7 (seven) working days, the Recipient provides a reply to the Whistleblower regarding the receipt and acceptance of the Report.

[6] If the Report concerns one of the Recipients, the management of the Report will be entrusted to the Recipient not involved.

The Recipient has the right, depending on the specific requirements, to involve other competent company functions (for example, HR, Internal Audit) with the purpose of managing the Report and/carrying out investigations. If the Report has any implications for the purposes of Legislative Decree 231/01, the Recipient also informs the Supervisory Body of SAES and the Company to which the Report refers and coordinates with the latter for the management thereof and for the conducting of the preliminary investigation. There will be no negative consequences suffered by anyone who has made a Report in good faith and the confidentiality of the identity of the Whistleblower and the reported person is ensured (within the limits of the provisions of the Regulations and the applicable laws).

7.2 With reference to the Whistleblowing portal, the Whistleblower is informed, through the platform, of the filing of the Report or its acceptance. To this end, it is important for the Whistleblower to keep the identification code of the Report, which is automatically generated by the system once the Whistleblowing form has been completed. This is the only way to be able to communicate with the Recipient, obtain feedback on the status of the Report and carry out investigations in a detailed and precise manner. The identification code of the Report has an expiry date of 97 days, at the end of which the Whistleblower will no longer be able to access the Report.

Whistleblowers are reminded to periodically access the Report to check its progress and/or to respond to any requests for information from the Recipient necessary for carrying out the investigations.

9. Investigations

The Recipient, after receiving and taking charge of the Report, conducts a preliminary assessment of the same, concerning, in particular, the relevance of the facts reported and their suitability for being reported on the basis of what is required by the Regulations.

The Recipient, after completing the aforementioned examination, closes the Report if it considers that the Report does not fall within one of the cases provided for by the Regulations (e.g. if it is a personal complaint), or if:

a) the Report is clearly unfounded or made in bad faith,
b) the facts reported have already been verified,
c) the Report is not substantiated (if additional elements are not provided or those provided are not sufficient and the Whistleblower does not provide any additional elements requested) and therefore not verifiable.

In other cases, the Recipient will verify the validity of the circumstances represented in the Report, in compliance with the principles of impartiality and confidentiality, carrying out all activities deemed appropriate, involving the competent corporate functions. The investigation activity[7] consists of the following phases:

a) *action plan* during which the investigation methods are defined, along with the resources to be involved;

[7] As regards Reports sent by e-mail, acceptance of the request as well as requests for further information by the Recipient from the Whistleblower take place through the reciprocal exchange of e-mails.
It is understood that the information exchanged between the various parties is also tracked within the Whistleblowing portal by the Recipient.

b) the conducting of the investigation itself, including through the collection and analysis of documents, interviews, etc .;
c) *reporting* and *remediation*, through follow-up activities to the Whistleblower, final report and indication of any remedial actions.

The Recipient provides a response to the Report within 90 (ninety) days from the date of receipt or, in the absence of such notice, within 90 (ninety) days from the expiry of the term of 7 (seven) days from the date of submission of the Report. In complex cases, it may be possible to extend the duration of the investigation subject to notification to the Whistleblower, via the Platform and e-mail.

If the report is found to be justified, any measures deemed appropriate will be taken. If, at the end of the investigation, the Report is found to be well-founded, the Recipient, according to the nature of the violation, may a) communicate the outcome of the assessment: a) to the Manager of the Structure to which the alleged perpetrator belongs, so that s/he may adopt the relevant management measures, including, if the conditions are met, the imposition of disciplinary action (in coordination with the HR Function); b) the Company Management and the competent structures to take any further measures and/or actions (which may include complaints/reports) that are necessary in the specific case to protect the Company and the SAES Group.

At the end of the investigation, the Receiver shall inform the Whistleblower through the Reporting platform and/or by e-mail in the case of Reports by e-mail.

The Recipient responds to the Reports received, the validity of which has been ascertained and for which an action plan has been proposed and implemented, to the Supervisory Body of SAES and the companies of the SAES Group concerned, in relation to their respective duties and responsibilities.

10. Storage of the documentation relating to the Report

The Register of Reports (i.e. the database of Reports stored on the platform) and the confidential information contained therein are accessible only to the Recipient.
The Reports and the related documentation will be kept on the Platform for 90 (ninety) days from the date of receipt or, in the absence of such notice, for 90 (ninety) days from the expiry of the term of 7 (seven) days from the date of receipt, starting from the date of submission of the Report; once this deadline has elapsed, they will be deleted from the Platform/e-mail, unless the investigation has been extended, as regulated in Article 9 above. Some summary data of the Report (which also include personal data) are kept for a period not exceeding 5 (five) years from the date of communication of the final outcome of the Report procedure, for requirements related to the definition of any (internal) and/or external proceedings) initiated as part of the Report and/or for the exercising of the right of defence in the event of disputes. This is without prejudice to retention for a longer period in relation to requests from the Public Authority (e.g. Legal Authorities).

11. Protection of the Whistleblower

SAES prohibits retaliatory or discriminatory acts of any kind, whether direct or indirect, against the Whistleblower for reasons connected, directly or indirectly, to the Report or to those who have cooperated in activities to verify the validity of the Report.
SAES guarantees the anonymity of the Whistleblower (if requested by the Whistleblower), including in cases of general information indicated, and specifies that the sanction system adopted is to be understood as integrated with the following provisions that may be applied against anyone who implements or threatens

to impose acts of retaliation against those who have submitted Reports under this policy or against those who, with wilful misconduct or gross negligence, have made Reports that have proven to be unfounded.

Disciplinary measure	Disciplinary violation
• ***Written admonishment***	Any minor misconduct giving rise to conduct not in line with the provisions of Italian Legislative Decree 231/2001 and with this policy.
• ***Fine not exceeding three hours' pay***	An employee who violates the internal procedures laid down in the Model or whose conduct does not comply with the provisions of the Organisation Model or this policy shall be liable to a fine not exceeding 3 hours' pay or to suspension from work for up to 3 days, depending on the seriousness of the violation, in the event of misconduct that is likely to be detrimental to the Company's rules, ethics, hygiene and safety, pursuant to the applicable NCLA.
• ***Suspension from work and pay up to a maximum of three days***	
• ***Dismissal with notice***	Workers who, in performing their activities, engage in conduct that violates the provisions of the Organisation Policy or this policy and which may lead to applying the sanctions provided for by Italian Legislative Decree 231/2001 against the company and/or in any case conduct likely to cause serious moral and/or material damage to the Company, pursuant to the provisions of the applicable NCLA, shall be dismissed.
• ***Dismissal without notice***	

It should be noted that the instances of misconduct listed do not include all possible misconduct liable to sanctions, with the list provided for purely illustrative purposes.

Pursuant to the provisions of the Regulations, the regime of protection measures envisaged to protect the Whistleblower applies only if:

a) at the time of the Report or the complaint or public disclosure, the Whistleblower had reasonable grounds to believe that the information on the violations - as reported, publicly disclosed or declared - was true and fell within the objective scope of Legislative Decree No. 24/2023;
b) the Reporting or public disclosure was carried out on the basis of the provisions of Italian Legislative Decree No. 24/2023.

Furthermore, from a general standpoint, the Company reserves the right to assess each individual behaviour and apply the most appropriate disciplinary measure (regardless of the measures indicated by way of example in the tables), depending on the severity of the event and in relation to the role and duties performed by the workers concerned and to the specific context in which the relevant conduct was

committed. The objective severity of the event and the degree of intent will be taken into account, in view of the fact that the Disciplinary Code is not to be considered as offering preferential treatment with respect to the NCLA applied.

12. Responsibilities of the Whistleblower

It is the Whistleblower's responsibility to make Reports in good faith and in line with the declared spirit of the project: Reports that are patently false or totally groundless, opportunistic and/or submitted with the sole aim of harming the reported party or other persons concerned by the Report will be disregarded.

It should be noted that this procedure is without prejudice to the criminal and disciplinary liability of the Whistleblower in the event of a slanderous or defamatory Report, or his/her civil liability for the same reason in cases of wilful misconduct or gross negligence; in these cases, the protections envisaged by the Regulations are not guaranteed to the Whistleblower. Any forms of abuse of this policy, such as patently opportunistic Reports and/or those made for the sole purpose of damaging the reported person or other parties, and any other case of improper use or intentional exploitation of the arrangement established under this procedure will also render the perpetrators liable.

The identity of the Whistleblower must never be disclosed to the reported person, except in the cases provided for by law, in order to avoid retaliation, threats, violence, etc. and protect the confidentiality of the latter. Given the above, where there is a substantial risk that disclosure of the relevant information will compromise the ability to effectively verify the validity of the Report or gather the necessary evidence, the reported person may not be informed of the recording of his/her Data, as long as this is necessary to guarantee the correct management of investigations and in any case in compliance with the provisions of the applicable national collective agreement. Under no circumstances may the reported person make use of his/her right of access to obtain information on the identity of the Whistleblower, unless s/he has made a Report in bad faith.

The identity of the Whistleblower and any other information from which this identity may be inferred, directly or indirectly, may not be disclosed, without his/her express consent, to persons other than those competent to receive or follow up on Reports, expressly authorised to process such data pursuant to privacy laws.

13. Rights of the reported person

During the verification and ascertainment of possible non-compliance, the individuals subject to the Reports could be involved in or notified of this activity, but under no circumstances will proceedings be initiated solely on the basis of the Report, in the absence of concrete feedback regarding the content thereof. This could possibly take place on the basis of other evidence found and ascertained from the Report itself, in compliance with current legislation.

The identity of the persons involved and the persons mentioned in the Report is protected until the conclusion of the proceedings initiated by virtue of the Report in compliance with the same guarantees envisaged in favour of the Whistleblower.

14. Applicability of the Policy to SAES Group companies

This Policy also applies to the SAES Group companies; in particular, a) to Italian companies that have adopted a Model pursuant to Legislative Decree no. 231/2001 within the limits of the provisions of the Regulation, and b) to foreign companies, with reference to violations of Group codes, company procedures and laws and regulations, to the extent that they are compatible with the applicable local regulations.

15. Communication, training and refresher sessions

This policy is published on the Company's website, in the dedicated section.

The Company has implemented training activities for its personnel on the Whistleblowing regulations and will communicate any updates to this policy.

16. Privacy Policy

16.A The following Privacy Policies are related to the processing of personal data carried out by the SAES Group companies governed by Italian law which falls within the scope of application of the Regulation (as mentioned below), as data controllers.

The processing of personal data as part of the Reports will take place in compliance with the legislation on personal data protection and any other applicable laws and/or regulations. **Therefore, we invite you to carefully read this information on the processing of personal data**.

***i)* Privacy Policy - SAES Coated Films S.p.A.**

A. The data controller of personal data is SAES Coated Films S.p.A., with registered office in Roncello (MB) via Leonardo da Vinci 3, tax code and VAT No. 03343590968 ("***SCF***").

B. Type of Data collected and processed. As part of the management of Reports, all personal data contained therein (the "***Data***") will be processed. The Data may refer to the Whistleblower, where the Report includes his/her name, to the subject(s) reported and/or to any third parties, where mentioned in the Report itself.

The processing of the Data may therefore concern, in addition to common personal data, also sensitive personal data or those that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data intended to uniquely identify a natural person, data relating to the health or sex life or sexual orientation of the person. Sensitive data are those belonging to the "special categories" pursuant to art. 9 of Regulation (EU) 679/2016 (GDPR).

These data will be processed exclusively where strictly necessary in order to manage the Report, in compliance with the principles of proportionality and necessity.

C. Purpose of data processing and related legal basis. The processing will take place in order to manage, process, investigate and resolve the Report, as well as to establish any disciplinary measures or otherwise adopt the measures appropriate to the case in question. The implementation of a tool and a policy to be followed for reporting meets the specific needs of internal control of the company and monitoring of company risks, specifically dictated by law.

This legal basis of the processing is the need to manage the Report and to fulfil the related legal obligations, as well as the legitimate interest of SCF in the implementation of an adequate Whistleblowing system.

D. Data Processor and Designated Subjects. For the aforementioned purposes, the Data may be accessible to the parent company SAES Getters S.p.A. (which manages the SAES Group's Whistleblowing system and will process them as the data controller, designated by SCF through a specific agreement), as well as to the Whistleblowing platform provider (who has been duly appointed by SAES as data processor by virtue of a specific written assignment, granted by SAES itself).

The Recipient (as well as any other parties who may have access to the Report for the management of the same) will process the Data as the designated party to receive the Reports, by virtue of a specific signed deed of appointment.

E. Data processing methods. In relation to the indicated purposes, the Data will be processed using manual and/or electronic tools, which ensure the protection of the data by design and by default, adequate to guarantee its security and confidentiality, and with logic strictly related to the purposes themselves, by parties to whom SAES has given adequate operating instructions with particular reference to the security measures adopted.

In relation to the processing in question, SCF also carried out an impact assessment on the protection of the Data, which showed that the processing of the Data does not present a high risk for the rights and freedoms of natural persons. For any information on the impact assessment, you can contact us by writing to privacy@saes-group.com or by contacting the Legal & Compliance Office at SAES Getters S.p.A. by writing to Viale Italia 77, Lainate (MI).

F. Provision of Data. The provision of personal data relating to the reported party for purposes relating to the management of Reports is strictly necessary. Failure to provide the data of the reported party will make it impossible to carry out the verification activities described above. The provision of the Whistleblower's personal data is, on the other hand, optional.

G. Disclosure of Data. The Personal Data contained in the Reports, if necessary, for example, for the management and assessment of the Report or for the activation of disciplinary protection related to the Report, may be communicated, subject to the consent of the Data Subject, to persons other than those competent to receive or to follow up on Reports, expressly authorised to process such data pursuant to arts. 29 and 32(4) of the GDPR and article 2-quaterdecies of the personal data protection code pursuant to Italian Legislative Decree no. 196, as subsequently amended and supplemented.

This is without prejudice to legal obligations and the protection of the rights of the data controller or persons (natural or legal) in any case concerned by and/or involved in the Report.

H. Data Retention. The personal data collected as part of a Report are retained for 90 (ninety) days from the date of receipt or, in the absence of such notice, for 90 (ninety) days from the expiry of the term of 7 (seven) days from the date of receipt, starting from the date of submission of the Report, unless the investigation is extended. Some summary data of the Report (which also include personal data) are retained for a period not exceeding 5 (five) years[8] (starting from the date of communication of the final outcome of the Report procedure) for requirements related to the definition of any proceedings (internal and/or external) initiated as part of the Report and/or for the exercising of the right of defence in the event of disputes. This is without

[8] For Reports made before the entry into force of this procedure, the retention period identified is 10 years (as envisaged in the previous version of the Privacy Policy and the procedure).

prejudice to retention for a longer period in relation to requests from the Public Authority (e.g. Legal Authorities).

I. Transfer of Data abroad. Any personal data may be transferred outside national territory (including outside the European Union) in order to process the Report. In any case, this transfer will take place in compliance with the reference legislation, providing for adequate guarantees, subject to the adoption of the necessary measures to ensure a level of protection similar to that guaranteed within the European Union.

L. Rights of the data subject At any time, the data subject may exercise the other rights recognised pursuant to the legislation on the protection of personal data in force and, in particular: the right to ask the data controller to confirm that the processing of data concerning the data subject, access to the data and the rectification or cancellation of the same or the limitation of data processing; the right to object to processing for one or more of the related purposes and/or in relation to one or more of the contact details provided; the right to data portability; the right to lodge an appeal with the Legal Authorities or a complaint with the competent Data Protection Authority.
The data subject may also request the complete list of recipients of the data at any time.
These rights may be exercised by writing to the e-mail address: privacy@saes-group.com or, by post, to Viale Italia 77, 20045 Lainate, Milan (for the attention of the Legal & Compliance Office of SAES Getters S.p.A.).
For information or clarifications on rights, or on the processing of personal data, the data subject may contact us at the same addresses.

***ii)* Privacy Policy - Strumenti Scientifici CINEL S.r.l.**

A. The data controller of personal data is Strumenti Scientifici CINEL S.r.l., with registered office in Vogonza (PD), viale dell'Artigianato 14/14-A, tax code and VAT No. 00857140289 ("***CINEL***").

B. Type of Data collected and processed. As part of the management of Reports, all personal data contained therein (the "***Data***") will be processed. The Data may refer to the Whistleblower, where the Report includes his/her name, to the subject(s) reported and/or to any third parties, where mentioned in the Report itself.

The processing of the Data may therefore concern, in addition to common personal data, also sensitive personal data or those that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data intended to uniquely identify a natural person, data relating to the health or sex life or sexual orientation of the person. Sensitive data are those belonging to the "special categories" pursuant to art. 9 of Regulation (EU) 679/2016 (GDPR).

These data will be processed exclusively where strictly necessary in order to manage the Report, in compliance with the principles of proportionality and necessity.

C. Purpose of data processing and related legal basis. The processing will take place in order to manage, process, investigate and resolve the Report, as well as to establish any disciplinary measures or otherwise adopt the measures appropriate to the case in question. The implementation of a tool and a policy to be followed for reporting meets the specific needs of internal control of the company and monitoring of company risks, specifically dictated by law.

This legal basis of the processing is the need to manage the Report and to fulfil the related legal obligations, as well as the legitimate interest of CINEL in the implementation of an adequate Whistleblowing system.

D. Data Processor and Designated Subjects. For the aforementioned purposes, the Data may be accessible to the parent company SAES Getters S.p.A. (which manages the SAES Group's Whistleblowing system and will process them as the data controller, designated by SCF through a specific agreement), as well as to the Whistleblowing platform provider (who has been duly appointed by SAES as data processor by virtue of a specific written assignment, granted by SAES itself).

The Recipient (as well as any other parties who may have access to the Report for the management of the same) will process the Data as the designated party to receive the Reports, by virtue of a specific signed deed of appointment.

E. Data processing methods. In relation to the indicated purposes, the Data will be processed using manual and/or electronic tools, which ensure the protection of the data by design and by default, adequate to guarantee its security and confidentiality, and with logic strictly related to the purposes themselves, by parties to whom SAES has given adequate operating instructions with particular reference to the security measures adopted.

In relation to the processing in question, CINEL also carried out an impact assessment on the protection of the Data, which showed that the processing of the Data does not present a high risk for the rights and freedoms of natural persons. For any information on the impact assessment, you can contact us by writing to privacy@saes-group.com or by contacting the Legal & Compliance Office at SAES Getters S.p.A. by writing to Viale Italia 77, Lainate (MI).

F. Provision of Data. The provision of personal data relating to the reported party for purposes relating to the management of Reports is strictly necessary. Failure to provide the data of the reported party will make it impossible to carry out the verification activities described above. The provision of the Whistleblower's personal data is, on the other hand, optional.

G. Disclosure of Data. The Personal Data contained in the Reports, if necessary, for example, for the management and assessment of the Report or for the activation of disciplinary protection related to the Report, may be communicated, subject to the consent of the Data Subject, to persons other than those competent to receive or to follow up on Reports, expressly authorised to process such data pursuant to arts. 29 and 32(4) of the GDPR and article 2-quaterdecies of the personal data protection code pursuant to Italian Legislative Decree no. 196, as subsequently amended and supplemented.

This is without prejudice to legal obligations and the protection of the rights of the data controller or persons (natural or legal) in any case concerned by and/or involved in the Report.

H. Data Retention. The personal data collected as part of a Report are retained for 90 (ninety) days from the date of receipt or, in the absence of such notice, for 90 (ninety) days from the expiry of the term of 7 (seven) days from the date of receipt, starting from the date of submission of the Report, unless the investigation is extended. Some summary data of the Report (which also include personal data) are retained for a period not exceeding 5 (five) years[9] (starting from the date of communication of the final outcome of the Report procedure) for requirements related to the definition of any proceedings (internal and/or external) initiated as part of the Report and/or for the exercising of the right of defence in the event of disputes. This is without

[9] For Reports made before the entry into force of this procedure, the retention period identified is 10 years (as envisaged in the previous version of the Privacy Policy and the procedure).

prejudice to retention for a longer period in relation to requests from the Public Authority (e.g. Legal Authorities).

I. Transfer of Data abroad. Any personal data may be transferred outside national territory (including outside the European Union) in order to process the Report. In any case, this transfer will take place in compliance with the reference legislation, providing for adequate guarantees, subject to the adoption of the necessary measures to ensure a level of protection similar to that guaranteed within the European Union.

L. Rights of the data subject At any time, the data subject may exercise the other rights recognised pursuant to the legislation on the protection of personal data in force and, in particular: the right to ask the data controller to confirm that the processing of data concerning the data subject, access to the data and the rectification or cancellation of the same or the limitation of data processing; the right to object to processing for one or more of the related purposes and/or in relation to one or more of the contact details provided; the right to data portability; the right to lodge an appeal with the Legal Authorities or a complaint with the competent Data Protection Authority.
The data subject may also request the complete list of recipients of the data at any time.
These rights may be exercised by writing to the e-mail address: privacy@saes-group.com or, by post, to Viale Italia 77, 20045 Lainate, Milan (for the attention of the Legal & Compliance Office of SAES Getters S.p.A.).
For information or clarifications on rights, or on the processing of personal data, the data subject may contact us at the same addresses.

16.B This Privacy Policy refers to the processing of personal data carried out by the parent company SAES Getters S.p.A. as data controller (therefore relating to all companies of the SAES Group not mentioned in the previous article 16.A i) and ii)).

***iii)* Privacy Policy - SAES Getters S.p.A.**

A. The data controller of personal data is SAES Getters S.p.A., with registered office in 20045 - Lainate (MI), Viale Italia 77, tax code and VAT No. 00774910152.

B. Type of Data collected and processed. As part of the management of Reports, all personal data contained therein (the "***Data***") will be processed. The Data may refer to the Whistleblower, where the Report includes his/her name, to the subject(s) reported and/or to any third parties, where mentioned in the Report itself.

The processing of the Data may therefore concern, in addition to common personal data, also sensitive personal data or those that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data intended to uniquely identify a natural person, data relating to the health or sex life or sexual orientation of the person. Sensitive data are those belonging to the "special categories" pursuant to art. 9 of Regulation (EU) 679/2016 (GDPR).

These data will be processed exclusively where strictly necessary in order to manage the Report, in compliance with the principles of proportionality and necessity.

C. Purpose of data processing and related legal basis. The processing will take place in order to manage, process, investigate and resolve the Report, as well as to establish any disciplinary measures or otherwise adopt the measures appropriate to the case in question. The implementation of a tool and a policy to be

followed for reporting meets the specific needs of internal control of the company and monitoring of company risks, specifically dictated by law.

This legal basis of the processing is the need to manage the Report and to fulfil the related legal obligations, as well as the legitimate interest of SAES in the implementation of an adequate Whistleblowing system.

D. Data Processor and Designated Subjects. For the aforementioned purposes, the Data may be accessible to third-party providers of ancillary services necessary for the management of Reports (e.g. platform provider). These subjects will process the Data, depending on the case, as independent controllers, or as data processors by virtue of a specific written assignment granted to them by SAES.

The Recipient (as well as any other parties who may have access to the Report for the management of the same) will process the Data as the designated party to receive the Reports, by virtue of a specific signed deed of appointment.

E. Data processing methods. In relation to the indicated purposes, the Data will be processed using manual and/or electronic tools, which ensure the protection of the data by design and by default, adequate to guarantee its security and confidentiality, and with logic strictly related to the purposes themselves, by parties to whom SAES has given adequate operating instructions with particular reference to the security measures adopted.

In relation to the processing in question, SAES also carried out an impact assessment on the protection of the Data, which showed that the processing of the Data does not present a high risk for the rights and freedoms of natural persons. For any information on the impact assessment, you can contact us by writing to privacy@saes-group.com or by contacting the Legal & Compliance Office at SAES Getters S.p.A. by writing to Viale Italia 77, Lainate (MI).

F. Provision of Data. The provision of personal data relating to the reported party for purposes relating to the management of Reports is strictly necessary. Failure to provide the data of the reported party will make it impossible to carry out the verification activities described above. The provision of the Whistleblower's personal data is, on the other hand, optional.

G. Disclosure of Data. The Personal Data contained in the Reports, if necessary, for example, for the management and assessment of the Report or for the activation of disciplinary protection related to the Report, may be communicated, subject to the consent of the Data Subject, to persons other than those competent to receive or to follow up on Reports, expressly authorised to process such data pursuant to arts. 29 and 32(4) of the GDPR and article 2-quaterdecies of the personal data protection code pursuant to Italian Legislative Decree no. 196, as subsequently amended and supplemented.

This is without prejudice to legal obligations and the protection of the rights of the data controller or persons (natural or legal) in any case concerned by and/or involved in the Report.

H. Data Retention. The personal data collected as part of a Report are retained for 90 (ninety) days from the date of receipt or, in the absence of such notice, for 90 (ninety) days from the expiry of the term of 7 (seven) days from the date of receipt, starting from the date of submission of the Report, unless the investigation is extended. Some summary data of the Report (which also include personal data) are retained for a period not

exceeding 5 (five) years[10] (starting from the date of communication of the final outcome of the Report procedure) for requirements related to the definition of any proceedings (internal and/or external) initiated as part of the Report and/or for the exercising of the right of defence in the event of disputes. This is without prejudice to retention for a longer period in relation to requests from the Public Authority (e.g. Legal Authorities).

I. Transfer of Data abroad. Any personal data may be transferred outside national territory (including outside the European Union) in order to process the Report. In any case, this transfer will take place in compliance with the reference legislation, providing for adequate guarantees, subject to the adoption of the necessary measures to ensure a level of protection similar to that guaranteed within the European Union.

L. Rights of the data subject At any time, the data subject may exercise the other rights recognised pursuant to the legislation on the protection of personal data in force and, in particular: the right to ask the data controller to confirm that the processing of data concerning the data subject, access to the data and the rectification or cancellation of the same or the limitation of data processing; the right to object to processing for one or more of the related purposes and/or in relation to one or more of the contact details provided; the right to data portability; the right to lodge an appeal with the Legal Authorities or a complaint with the competent Data Protection Authority.
The data subject may also request the complete list of recipients of the data at any time.
These rights may be exercised by writing to the e-mail address: privacy@saes-group.com or, by post, to Viale Italia 77, 20045 Lainate, Milan (for the attention of the Legal & Compliance Office).
For information or clarifications on rights, or on the processing of personal data, the data subject may contact us at the same addresses.

M. Data Protection Officer. SAES has appointed its own data protection officer, who can be contacted at the following addresses for information on data processing and on the rights granted to data subjects: LCA Servizi S.r.l., Gianluca De Cristofaro (email: dpo@saes-group.com; Tel. 02 7788751).

[10] For Reports made before the entry into force of this procedure, the retention period identified is 10 years (as envisaged in the previous version of the Privacy Policy and the procedure).