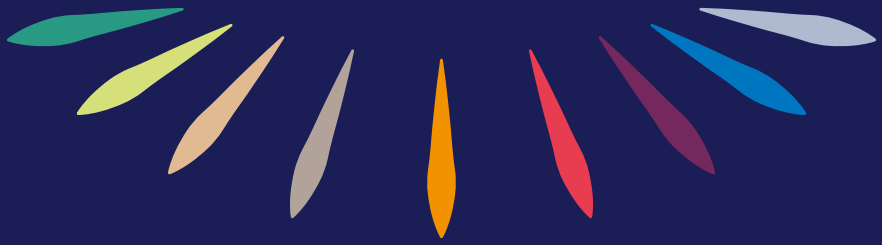
PROCEDURE FOR COLLECTING AND PROCESSING REPORTS AND ALERTS



SPIE, sharing a vision for the future

Failure to comply with the laws and regulations applicable to SPIE or SPIE's ethical rules may have serious consequences for SPIE and its employees.

The SPIE Group is committed to complying with and applying laws and ethical standards. It has set up a Code of Ethics

https://alert.spie.com/

as well as a Code of Ethics Implementation Guide for its employees.

If there are any doubts, questions or concerns regarding a situation or an issue concerning the application of the law or the Group's ethical standards, employees may contact their direct or indirect supervisor; the legal affairs department, the Group Legal and Insurance Department; Human Resources; Ethics Officers and Committees or employees' representatives.

Employees may also use the Group professional whistleblower system covered under this procedure.

The SPIE Group is committed to ensuring the confidentiality of the reports processed and prohibits any form of reprisal against employees who use the system.

Use of this system is optional and is additional to the traditional means of reporting. No sanctions may be imposed on any employee on the grounds that he or she has not made use of this system.

This system is open to SPIE employees, occasional or external workers and to stakeholders.

SPIE entities located outside France have to assess if, according to their national legislation, this procedure requires amendments in order to be complaint with mandatory domestic rules. They shall communicate locally about amendments applicable to the procedure.

NB: the terms "report" and "alert" are used interchangeably.

1. CONDITIONS RELATING TO WHISTLEBLOWERS

Only individuals may issue a report or alert.

Alerts and reports may be issued by all SPIE employees and all external or occasional employees: temporary staff; trainees; service providers' employees; employees of subcontracting companies and all interested parties (customers, suppliers' staff, SPIE shareholders).

All reports of an alert must be made:

- in good faith:
- and free from any personal interest of the whistleblower.

Whistleblowers must not act maliciously, with intent to harm or expect any personal or professional consideration or financial compensation for making a report.

They must have personal knowledge of the facts or acts they report (in other words, rumours, speculation and inferences are excluded).

2. PROTECTION OF WHISTLEBLOWERS

No employee who meets the conditions set out in section 1 of this procedure may be excluded from a recruitment procedure or from access to a traineeship or a period of professional training.

No person who meets the conditions set out in section 1 of this procedure may be:

- sanctioned;
- dismissed;
- directly or indirectly discriminated against, in particular in terms of remuneration, profit-sharing or share distribution measures, training, reclassification, assignment, qualification, professional promotion, transfer or contract renewal;

even if the alleged facts prove to be inaccurate or do not lead to any action.

Nevertheless, any person who misuses or uses this system in bad faith may face disciplinary sanctions or legal proceedings as the case may be.

Any information which could identify the whistleblower is confidential and may not be disclosed, except to the judicial authorities and only with the whistleblower's consent.

Employees who have made a report must identify themselves, but their identity is treated confidentially by the Group Compliance Officer in charge of managing alerts.

Anonymous reports must be avoided and will only be dealt with exceptionally if the seriousness of the facts is established and the factual elements are sufficiently detailed.

3. EVENTS THAT MAY BE REPORTED

- any misdemeanour or crime;
- any serious and manifest violation of an international commitment duly ratified or approved by France or by a country where SPIE has activities;
- any serious and manifest violation of a unilateral act of an international organisation taken on the basis of a regularly ratified international commitment;
- any serious and manifest violation of laws or regulations;
- any serious threat or harm to the general interest.

For example, a report may cover:

- violations:
  - of anti-corruption laws;
  - of competition law;
  - of banking law;
  - of securities law;
  - of accounting law;
- events likely to constitute:
  - internal or external fraud;
  - a safety risk;
  - misuse of corporate assets;
  - embezzlement of assets;
  - insider trading;
  - a conflict of interest

Elements potentially being a case of psychological or sexual harassment can be reported by the person considering to be subjected to such a situation.

No facts, information or documents relating to medical secrecy, national defence or attorney-client privilege may be the subject of a report.

The incidents may also involve a violation of the Code of Ethics or situations that are contrary to the Code of Ethics Implementation Guide for SPIE employees.

4. ISSUING ALERTS

Anyone wishing to make a report through the whistleblower system can do so by contacting:

- their direct or indirect superior;
- the Compliance Officer of their subsidiary;
- an employee representative;
- the Group Compliance Officer.

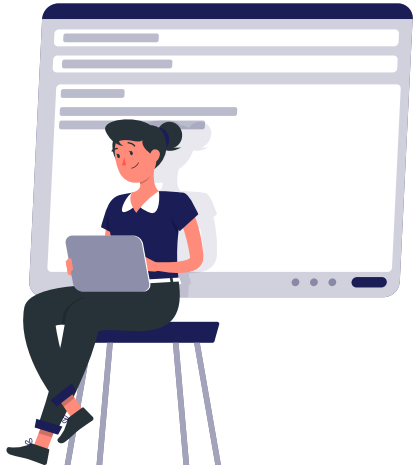
The report may be sent:

- by post: stating «CONFIDENTIAL» on the envelope and indicating in the subject line that it concerns an alert;
- or on the dedicated platform: https://alert.spie.com/
  This site is secure and managed by an external service provider that is bound by a strict duty of confidentiality. The Group Compliance Officer receives all alerts issued on this platform.

In order to ensure a high level of confidentiality and security, it is asked that all whistleblowers use the dedicated whistleblower platform as a preferred method of alerting.

It is recalled that elements and data that could identify whistleblowers may not be disclosed, except to the judicial authorities and only with the consent of the person concerned.

Whistleblowers must provide all facts, information, documents or data, in any form or medium, that might substantiate their reports when they are in possession of such information. Such facts, information, documents or data may simply be mentioned in the alert and made available to the recipient of the alert at short notice.



5. NOTIFICATION AND RIGHTS OF PERSONS WHO ARE THE SUBJECT OF AN ALERT

Any person who is the subject of alerts shall be notified by the recipient of the alert of any data concerning them as soon as the alert is recorded, even if the alert is not stored in electronic form.

The person may access said personal data and request that it be deleted or corrected if it is inaccurate, ambiguous or obsolete.

In the event that precautionary measures are necessary, in particular to prevent the destruction of evidence relating to the alert, the person concerned shall not be informed until after such measures have been adopted.

The recipient of the alert shall inform in writing any person targeted by an alert of the alleged acts, the services to whom the alert was sent and the procedures under which the person may exercise its rights to access and correct its personal data.

Under no circumstances may the person targeted by an alert be notified of the identity of the person issuing the alert.

No information that could identify the person implicated in an alert may be disclosed, except to the judicial authorities and only once the alert has been proven to be well-founded.

6. PROCESSING OF ALERTS

The recipient of the alert shall inform the sender of the alert in writing of its receipt and of the foreseeable time needed to assess whether it is admissible.

If the report does not fall within the scope of this procedure, is not of a serious nature, was made in bad faith or constitutes an abusive or slanderous allegation or concerns unverifiable facts, it shall be destroyed or archived after being rendered anonymous without delay and the whistleblower shall be notified accordingly.

As part of the processing of the alert, the recipient of the alert may carry out any investigations he or she deems necessary to ascertain whether or not the alert is well-founded.

He or she may call upon any employee whose assistance he or she deems necessary in connection with the verification or processing of the alert, it being understood that such employees shall be bound by an obligation of confidentiality.

Furthermore, the processing of the data that is collected shall be accessed through a regularly renewed individual user ID and password or by any other means of identification.

If warranted by the facts and if the recipient deems it necessary, he or she may appoint any external service provider with expertise in certain areas relevant to the investigation (for example, IT, finance, accounting).

This third party shall contractually undertake to comply with the strictest confidentiality requirements.

The whistleblower shall not take part in the investigations but may be asked to provide further details.

In particular, the processing of the alert shall be carried out in accordance with the principle that both parties should be heard and in accordance with applicable labour law.

7. CLOSING OF ALERT PROCESSING

The persons concerned by the alert will be notified of the closing of the alert processing operations.

Whistleblowers shall be informed of any action taken in response to their report to confirm if the reported facts are well-founded or not.

Upon completion of the processing of the alert, a decision will be taken on the action to be taken, such as any disciplinary measures or legal action under the applicable legal provisions.

8. DISSEMINATION OF THE PROCEDURE

This procedure shall be disseminated by any means that makes it accessible to permanent or occasional employees, and in particular through:

- electronic notification,
- posting on the boards reserved for this purpose,
- publication on the website and intranet.

9. PROTECTION OF PERSONAL DATA

In relation to a report, the whistleblower may communicate to SPIE personal data as well, as applicable, data concerning the persons targeted by the alert.

SPIE may also collect and process personal data of other persons in relation to the processing of an alert.

The nature of the data that could be collected and processed includes in particular:

- The identity, functions, and contact details of the whistleblower;
- The identity, functions, and contact details of the persons targeted by a report;
- Any other information voluntarily communicated by the whistleblowerоr or resulting from procession the alert.

SPIE guarantees the right of any person identified in the whistleblower system to access their personal data and to request, in the event that such personal data is inaccurate, incomplete, ambiguous or out of date, that it be corrected or deleted. These rights may be exercised by writing to rgpd.operations@spie.com.

Under no circumstances may persons who are the subject of an alert receive information concerning the identity of the sender of the alert in connection with their right of access to their personal data.

Information relating to an alert considered upon receipt as not being within the scope of this procedure are promptly archived after anonymization and subject to applicable laws for keeping records.

If the alert is within the scope of the procedure, the information provided through the alert shall be destroyed or archived within 2 months following the reached conclusion after processing the alert and subject to applicable laws for keeping records.

If the alert results in disciplinary measures or legal action, the information provided through the alert are kept for the duration of the procedure, subject to applicable laws for keeping records.

10. TRANSFER OF PERSONAL DATA OUTSIDE THE EUROPEAN UNION

In order to allow an alert to be processed, personal data may be transferred to the persons responsible for processing it in the relevant entities.

In the case of transfers of personal data to countries outside the European Economic Area (EEA) this transfer can only occur if the conditions defined in articles 45 to 50 of the European Regulation (EU) No 2016/679 are complied with by SPIE, including for subsequent transfers of personal data by a third country to another third country so that the level of protection of physical persons is not prejudiced.

www.spie.com

SPIE
Campus Saint-Christophe – Europa
10, avenue de l'Entreprise
95863 Cergy-Pontoise Cedex
FRANCE

SPIE_Ethic Code/Alerts - 11/2021 - Design and production: www.pastelle.fr