Ethics - Integrity - Compliance

Internal Alert
User guide to the internal alert system
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background to the user guide</td>
<td>4</td>
</tr>
<tr>
<td>Why use the internal alert system?</td>
<td>4</td>
</tr>
<tr>
<td>When to use the internal alert system?</td>
<td>5</td>
</tr>
<tr>
<td><strong>User guide</strong></td>
<td>6</td>
</tr>
<tr>
<td>Initiating an alert</td>
<td>6</td>
</tr>
<tr>
<td>Protection of individuals initiating an alert</td>
<td>8</td>
</tr>
<tr>
<td>Receipt, actionability assessment and handling of internal alerts</td>
<td>8</td>
</tr>
<tr>
<td>Identity of the individual raising an alert</td>
<td>10</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>11</td>
</tr>
<tr>
<td>Provisions applicable to individuals who are the subject of an alert</td>
<td>12</td>
</tr>
<tr>
<td>Provisions applicable to personal data</td>
<td>13</td>
</tr>
<tr>
<td><strong>Keeping in touch</strong></td>
<td>14</td>
</tr>
<tr>
<td>If you require more information or advice</td>
<td>14</td>
</tr>
<tr>
<td>To raise an alert</td>
<td>15</td>
</tr>
</tbody>
</table>
Thales has had an internal alert system in place for many years as part of its Code of Ethics. The Group is updating its internal alert system as a result of the entry into force of new regulations.

Why use the internal system?

The internal alert system was initially created to strengthen Thales’s approach to Ethics, Integrity and Corporate Responsibility, while giving employees a way to voice their concerns and play an active role in preventing risks.

It enables Thales employees, casual employees and external staff to report any acts that fall within the scope of the system.

The internal alert system is based on the principles of confidentiality and respect for the rights of each person concerned throughout the procedure.

Its use remains optional. No disciplinary action can be taken against any employee solely because they did not utilise the system.

When to use the internal system?

Subject to compatibility with local regulations, the internal alert system is designed to allow employees, casual employees and external staff to report concerns or incidents relating in particular to the following:

- Conduct or situations contrary to the Thales Code of Ethics, or the Group’s Code of Conduct - Prevention of corruption and influence peddling.
- A crime or offence.
- A serious and manifest violation of laws or regulations.
- A serious and manifest violation of an international undertaking from the French Republic (concerning for instance human rights and fundamental freedoms).
- A serious threat, or serious harm, to the public interest, of which the individual initiating the alert has personal knowledge.
- Serious abuses of human rights and fundamental liberties, and serious damage to the health and safety of persons and the environment, potentially resulting from the activities of Thales (and of its subcontractors and suppliers, where their activities meet the criteria laid down by regulations and case law).

In practice, such reporting may relate in particular to acts of corruption or influence peddling, discrimination, harassment, anti-competitive practices, breaches of stock market regulations, financial and accounting violations, etc.

---

1 However, if a country of operation has more stringent national legislation, the HR Department, the Ethics, Integrity and Corporate Responsibility Department and the Legal and Contracts Department will adapt this guide to ensure compliance with local laws and regulations.  2 Notably, in France, law No. 2016-1691 of 9 December 2016 on transparency, anti-corruption and the modernisation of the economy, law No. 2017-399 of 27 March 2017 on the duty of care of parent companies and companies using sub-contractors, and the European General Data Protection Regulation (GDPR).

3 This covers the activities of Thales (parent company) and/or of a company controlled directly or indirectly by Thales (parent company).  4 Alerts may not be raised, however, in respect of facts, information or documents (irrespective of their form or media) that fall within the scope of regulations governing the protection of national defence secrets, patient (medical) confidentiality or legal client privilege.
Initiating an alert

For an alert to be actionable, it must meet the following criteria:

- It must have been initiated by an employee, casual employee or member of external staff.
- It must fall within the scope of the system (see the different areas defined in the section “When to use the internal alert system”).
- It must relate to facts of which the individual initiating the alert has personal knowledge1.
- It must have been initiated in good faith and in an impartial manner2.

If an employee has doubts about acts or behaviours of which they have personal knowledge, they must alert their (direct or indirect) line manager, or their local ethics and/or compliance officer.

The role of line managers is to guide and advise their team members. Line management is therefore the preferred route for raising alerts. However, if informing (direct or indirect) line management would potentially cause difficulties, alerts may be raised via the internal alert system.

Thales provides the assurance that no reprisals will be taken against any employee who reports, in good faith and in an impartial manner, acts that fall within the scope of the internal alert system, even if the facts are subsequently shown to be incorrect, or do not give rise to any follow-up action.

Alerts must be raised in good faith. In other words, at the time when the individual initiates the alert, the acts reported must appear to fall within the scope of the alert system, such that the individual cannot be accused after the fact of seeking to harm others. Even if the facts are subsequently shown to be incorrect, alerts raised in good faith will not lead to any disciplinary action for the individual raising them.

However, any individual knowingly making false allegations cannot be considered to be acting “in good faith”. He/she may be then subject to disciplinary action and liable to prosecution under slander/libel legislation3.

Alerts may be reported by any means (by letter, email, telephone or in person) to the VP Ethics, Integrity and Corporate Responsibility. Dedicated contact details are as follows:

- Email: alert.thales@thalesgroup.com (or use the dedicated Intranet page)
- Phone: +33 1 57 77 87 19
- Postal address: Thales VP Ethics, Integrity and Corporate Responsibility Internal alert system Tour Carpe Diem 31 place des Corolles CS 20001 92098 Paris La Défense cedex FRANCE

Individuals must not, therefore, report acts observed by others, but must only report acts that they themselves have personally observed, and which they reasonably believe constitute acts that fall within the scope of the internal alert system. -

The individual initiating the alert shall not receive any benefit or remuneration in return for making the report. - 3In France, provision is made for such prosecution under article L 226-10 of the Code Penal.
Protection of individuals initiating an alert

Thales undertakes not to dismiss, discriminate against or otherwise take disciplinary action against any employee who initiates an alert for the purpose of reporting in good faith and in an impartial manner any acts falling within the scope of the internal alert system as defined above. Depending on the individual country, individuals initiating alerts may be protected under specific legislation.

Receipt, actionability assessment and handling of internal alert

Personal data collected is intended for use by the Ethics, Integrity and Corporate Responsibility Department, the Legal and Contracts Department, the members of the Alert Monitoring Committee, and the persons responsible for processing an alert, provided that they are required to access the information on a “need-to-know” basis for the purpose of verifying or processing an alert report.

All alerts received are acknowledged in writing by means of a message sent to the individual raising the alert.

Reviewing alerts to determine actionability

Alerts received are the subject of a confidential review, within a maximum of 15 calendar days, by the VP Ethics, Integrity and Corporate Responsibility (or his/her deputy) who shall consult the SVP, Legal and Contracts (or his/her deputy) to determine whether they are actionable.

Following this review, the VP Ethics, Integrity and Corporate Responsibility (or his/her deputy) sends an email to the individual who raised the alert to notify them of the outcome of the review (i.e. whether the alert is actionable or not).

Processing of alert

If an alert is declared actionable, the VP Ethics, Integrity and Corporate Responsibility (or his/her deputy) sets up with the SVP, Legal and Contracts (or his/her deputy) an Alert Monitoring Committee, whose composition varies depending on the area concerned.

The Alert Monitoring Committee appoints the individuals responsible for handling the alert, and decides whether to have investigations conducted internally or by a third-party body.

As far as possible, the VP Ethics, Integrity and Corporate Responsibility (or his/her deputy) informs the individual who raised the alert of the follow-up action taken in respect of the alert, provided that such information does not hinder the implementation of precautionary measures and/or the conduct of investigations.

If no follow-up action is taken in respect of an alert, the VP Ethics, Integrity and Corporate Responsibility (or his/her deputy) informs the individual who raised an alert and, where applicable, the person(s) who are the subject of the alert report, by email, that the alert procedure has been closed.

Following closure of an alert procedure, the Alert Monitoring Committee determines the appropriate means for ensuring that the employee is not subject to disciplinary action or discrimination as a result of having made a report in accordance with the internal alert procedure.

Retention of data

Personal data pertaining to an alert are destroyed, or archived after anonymization, in accordance with the time limits provided for under current regulations.

Data subject to archiving requirements are retained in a separate, restricted-access information system for a period that does not exceed the period provided for under current regulations.

---

1 In France, article L.1132-3-3 of the Labour Code (Code du travail) specifies: “No person may be excluded from a recruitment process or refused access to an internship or vocational training course, and no employee may be subject to disciplinary action, dismissed or subject to direct or indirect discriminatory measures, notably measures relating to remuneration as defined by Article L. 3221-3, or to profit-sharing or share awards, training, reassignment, assignment, qualification, classification, professional promotion, internal transfer or contract renewal, as a result of their having raised an alert in accordance with Articles 6 to 8 of law No. 2016-1691 of 9 December 2016 on transparency, anti-corruption and the modernisation of the economy.”
Identity of individual raising an alert

Except where local legislation makes provision to the contrary, the individual raising an alert is invited to disclose their identity in order to ensure more effective handling of the alert report by enabling additional details to be requested from them. In addition, if the identity of the individual raising an alert is known, measures can be put in place to ensure their protection.

However, even in the event of an anonymous alert, the reported facts will be examined to verify whether they are supported by evidence. Anonymous alerts can therefore be processed under the following conditions:

- The reported facts have been shown to relate to a sufficiently serious matter (such as harassment, corruption and influence peddling, for example).
- The factual information provided is sufficiently precise to allow verification to be carried out, or, if this is not the case:
- The individual who has raised the alert has provided information which allows discussions to take place with a view to obtaining further information, where applicable.

Confidentiality

Thales undertakes to implement procedures to guarantee that the identity of the individual raising an alert, the facts of the alert report, and the identity of the person(s) who are the subject of the alert report, are kept confidential, including in the event of disclosure to third parties.

Employees who use the internal alert facility can therefore be sure that every precaution will be taken to ensure that their identity is kept strictly confidential at every stage of the investigation and handling of the situation by all those who have access to information on alert reports.

Electronic documents are stored in a separate, restricted-access information system, open only to the VP Ethics, Integrity and Corporate Responsibility (or his/her deputy), the SVP, Legal and Contracts (or his/her deputy), and other potential members of the Alert Monitoring Committee, and to persons responsible for processing alerts, provided that they need to access the documents on a “need-to-know” basis for the purpose of verifying or processing an alert.

If necessary, exchanges via email with the individuals concerned by an alert can take place via an encrypted messaging system, the access arrangements for which will be provided once the alert has been declared actionable.

Only the VP Ethics, Integrity and Corporate Responsibility, the SVP, Legal and Contracts, and other potential members of the Alert Monitoring Committee will, in the first instance, be aware of the identity of the individual who initiated the alert. Disclosure of the identity of the individual who initiated the alert to other persons (with the exception of the judicial authority) is subject to the individual’s approval. In addition, information that could identify the person who is the subject of an alert report may only be disclosed (except to the judicial authority) once the actionability of the alert has been determined.
Provisions applicable to individuals who are subject of an alert

Individuals who are the subject of an alert report are informed of the existence of such a report as soon as data pertaining to them are recorded, unless precautionary measures are necessary, in particular to prevent the destruction of evidence relating to an alert, or to organise the protection of the individual initiating an alert against any reprisals. In such cases, the information will be provided to the person who is the subject of the alert report at the same time as, or after, such measures are adopted.

In any event, and subject to compliance with the provisions above, individuals who are the subject of an alert report must be informed of the following:

- The entity responsible for processing the alert.
- The substance of the allegations, together with an explanation of the individual’s right to respond.
- The persons, departments or entities who will have access to the data concerning the alert report, and are responsible for the investigations.
- How they can exercise their rights, subject to applicable legislation (access to personal data, correction, deletion, objection on legitimate grounds, etc.).

The individual initiating an alert, and individuals who are the subject of an alert report, where applicable, have rights of access, correction, deletion, restriction of processing, objection and portability in relation to data pertaining to them\(^1\). These rights can be exercised by sending an email to the dedicated email address:

alert.thales@thalesgroup.com.

---

\(^1\) - In accordance with Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
If you require more information or advice, contact:

Thales Ethics, Integrity and Corporate Responsibility Department
alert.thales@thalesgroup.com
Phone: + 33 (0)1 57 77 82 07

To raise an alert, contact:

If you encounter difficulties in performing your duties, first contact your manager, your HR manager or employee representative.

Alerts raised via the internal alert system may be reported by any means (by letter, email, telephone or in person) to the VP Ethics, Integrity and Corporate Responsibility. Dedicated contact details are as follows:

• Email: alert.thales@thalesgroup.com or use the dedicated Intranet page.
• Phone: +33 1 57 77 87 19
• Postal address: Thales VP Ethics, Integrity and Corporate Responsibility Internal alert system Tour Carpe Diem - 31 place des Corolles - CS 20001 92098 Paris La Défense cedex France