

# THE PROFESSIONAL ALERT SYSTEM AT SAINT-GOBAIN

Practical Guide  
July 2018



- 1. Who can issue an alert?
- 2. What is the scope?
- 3. How to issue an alert?
- 4. What are the admissibility requirements for an alert?
- 5. Who receives and handles the alerts?
- 6. How is confidentiality ensured?
- 7. How are the alerts handled?
- 8. What rights do the persons concerned by the alert have with regard to the processing of their personal data?
- 9. How are the data saved?
- 10. How is the issuer protected?

Legal protection of whistle-blowers  
In summary  
Who to contact?  
Resources



In 2011, the Group adopted a professional alert system allowing Saint-Gobain staff and external or occasional employees to report, in good faith, serious breaches of the law or of Group internal rules and regulations. In 2017, 211 alerts were issued.

Today, to make our employees more aware of this alert system and maximize its effectiveness, we have described hereunder the procedure to follow. Suppliers of the Group have now access to this alert system. This procedure is available in the **Compliance section** of the eWorkplace and will be relayed by the Sectors, Delegations and Purchasing teams.

Your direct superiors, the Human Resources Department and your legal teams are on hand to answer your questions. Feel free to contact them!

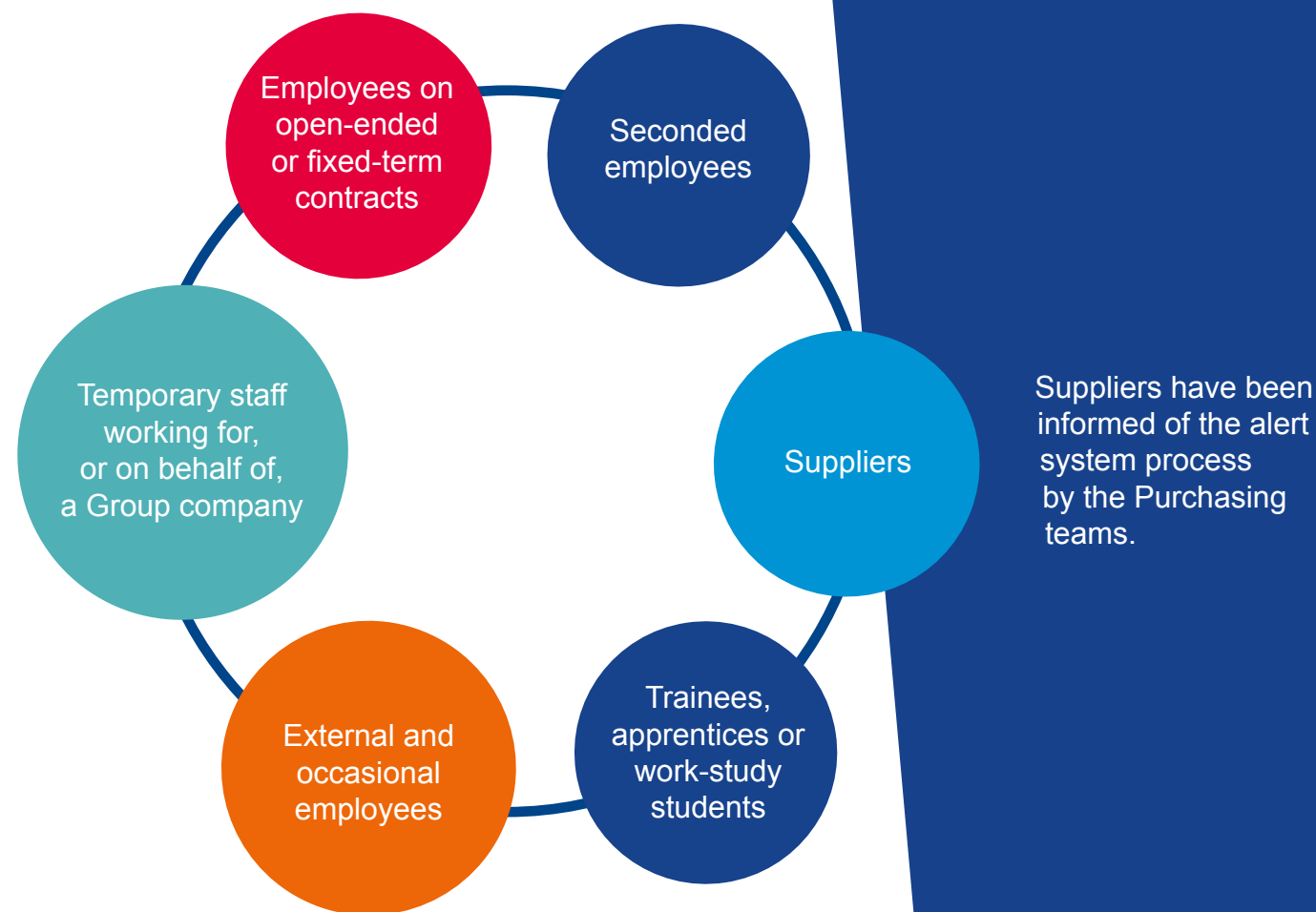
We hope this document proves to be both interesting and useful.

Antoine Vignial,  
General Secretary, in charge of Corporate Social Responsibility.

## 1. Who can issue an alert?

- The Group's professional alert system is available to all Saint-Gobain Group personnel and to external and occasional employees (employees on open-ended or fixed-term contracts, trainees, apprentices or work-study students, temporary staff working for, or on behalf of, a Group company, seconded employees...).

Who can have access to the Saint-Gobain's professional alert system?



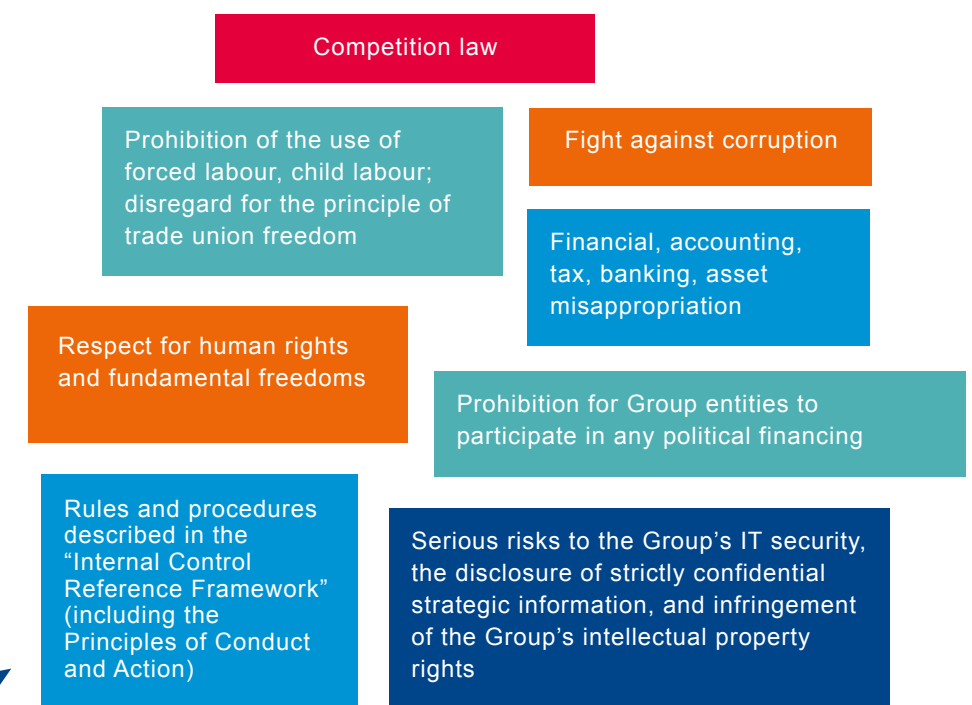
## 2. What is the scope?



- Under the alert system, it is possible to report potential breaches that would constitute:

- a crime or an offence,
- a serious and manifest breach of an international undertaking or obligation,
- a serious and manifest breach of the law or a regulation,
- a threat or serious damage to the general interest.

- This may include breaches in the following areas:



The Principles of Conduct and Action are the Saint-Gobain's code of conduct.



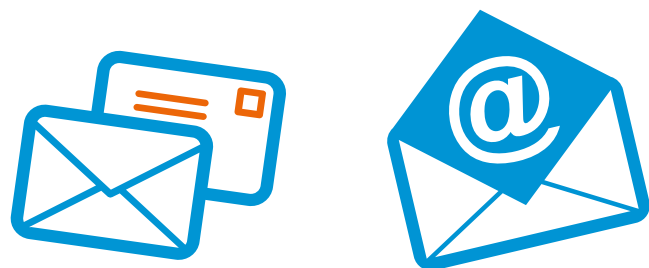
- However, an alert may not be related to elements which are classified or covered by professional secrecy, i.e. the legal privilege applicable to communications between lawyers and clients, or medical confidentiality.

### 3. How to issue an alert?

- ▶ Saint-Gobain's professional alert system is optional: no penalty or sanction may be imposed on a person not using this system even though entitled to do so.
- ▶ The alert system is a complementary way of reporting misconduct. It does not replace the other channels existing inside a company (hierarchy, Human Resources department, legal teams...).
- ▶ Any employee wishing to issue an alert must send an email from his/her personal Saint-Gobain email address to the dedicated email box. The current list of email boxes for France and for each Delegation is available within the **Compliance section** of the Group's eWorkplace and is appended to this Policy (see in Appendix).
- ▶ Persons without a Saint-Gobain email address can still issue an alert by sending a letter to the following address:

General Secretary  
Compagnie de Saint-Gobain  
Les Miroirs,  
18 avenue d'Alsace  
92400 Courbevoie, France

- ▶ The alert will only be considered if it complies with the admissibility requirements defined in paragraph 4 below.



One Group alert system.

Two ways to issue an alert:  
• by email  
• by mail

### 4. What are the admissibility requirements for an alert?

- ▶ The breach must be serious, and the alert must be issued in good faith, and selflessly.

The alert must describe objectively, and as precisely as possible, the facts that the issuer personally suffered or personally witnessed, including, if possible, the relevant dates, the entity concerned, and the names of the persons involved.

The issuer, or whistle-blower, provides information and documents to support the alert, regardless of their format.

In addition to the Group system, some countries may have chosen to use an external system with a third party.

In that case, either system (external or Group) may be used.

An issuer using both systems must indicate this.



## 5. Who receives and handles the alerts?

- ▶ Alerts are received by the people designated below who, due to their position, have the competence, authority and sufficient resources to carry out their duties (“the Officers”).

The Officers are:

- For France: the Group General Secretary and the Group Director of Internal Audit and Business Control;
- For others countries: the Group General Secretary, the Group Director of Internal Audit and Business Control, the General Delegate and the Compliance correspondent of the Delegation concerned.

The Officers undertake to comply with the principles detailed below.



When an alert is issued, an Officer is appointed to ensure that proceedings run smoothly.

The Officers are in charge of running the procedure smoothly and communicating with the issuer.

The Officers are subject to the following obligations:

- Confidentiality
- Independence and impartiality
- Transparency

The Officers may designate trustworthy people to assist them. These people shall be bound by the same obligations.

## 6. How is confidentiality ensured?

- ▶ The Saint-Gobain Group’s professional alert system is not anonymous. Nevertheless, the Officers undertake to treat the identity of the issuer, the information and documents received, as well as the identity of the persons targeted by the alert, with the strictest confidentiality.

However, such confidentiality must not impede or jeopardize the verification and handling of the alert. If handling an alert requires disclosing some information to the competent services of the Group or to third parties, only those details which are necessary for assessing the facts and dealing with the alert will be communicated, taking the following precautions:

- any details which may reveal the whistle-blower’s identity will only be disclosed once the issuer’s consent has been given;
- any details which may reveal the identification of the person targeted by the alert will only be disclosed once the admissibility of the alert has been established.

In any event, confidentiality may not be opposed to judicial authorities or regulators, nor impede possible disciplinary or judicial procedures.



## 7. How are the alerts handled?

- ▶ The Officers acknowledge receipt of the alert to the issuer. They inform the issuer of the foreseeable time required to examine the admissibility of the alert.



### Step 1: Acknowledgment of receipt

The acknowledgment of receipt sent to the issuer contains a reference number that is used to register the existence and the follow-up of the alert. It does not mean the alert is admissible.

If it is obvious that the alert is not admissible (see [paragraph 2](#) and [paragraph 4](#)), then the Officers shall notify the issuer of the alert and close the procedure.

Otherwise, the Officers appointed:

- send a questionnaire to the issuer that must be completed in order to collect additional information/documents;
- inform the issuer of the expected time required to examine the admissibility of the alert.

### Step 2: Handling of the alert on the basis of the questionnaire

- The issuer must return the questionnaire completed within 4 weeks. Otherwise, the procedure shall be closed, unless the reported allegations are particularly serious and sufficiently detailed to open an investigation.
- On the basis of the completed questionnaire, the Officers determine whether the alert is admissible and inform the issuer.

If the alert is not admissible (see [paragraph 2](#) and [paragraph 4](#)), the procedure is closed.

If the alert is admissible, then it is treated by the Officers.

- ▶ Then, the Officers review the reported facts described in the alert.



- ▶ If appropriate, they inform the persons targeted by an admissible alert of the facts relating to them. When precautionary measures need to be taken, especially to prevent the destruction of evidence, the persons are informed only after such measures have been implemented.

The Officers conduct the necessary investigations and verifications of the admissible alerts, and analyse their nature and severity.

► On this basis, they decide what actions should be taken and inform the issuer.

► Once the alert has been handled, the Officers inform the alert issuer, and if appropriate the persons targeted, of the closure of the alert.

► Exchanges with the alert issuer, if any, are made via the dedicated email box and each Officer shall retain information, ensuring the traceability of the alerts issued.



A follow-up of the alerts is ensured by the Group Compliance Committee.

## 8. What rights do the persons concerned by the alert have with regard to the processing of their personal data?

► The persons concerned by the alert may exercise all the rights they have under the applicable data protection regulation, and in particular their right to access, rectify or delete data, to restrict processing related to the person concerned, to oppose for legitimate reasons the treatment of the data, and to lodge a complaint to a supervisory authority.

Under no circumstances may a person targeted by an alert obtain, on the basis of their right to access data, any information regarding the identity of the alert issuer.

Personal data are protected in accordance with applicable local law on data privacy.





## 9. How are the data saved?

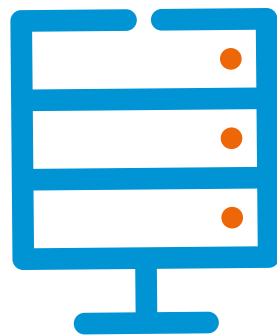
► The elements relating to non-admissible alerts are destroyed as soon as possible, or archived after being anonymized.

► For admissible alerts:

- When no disciplinary or judicial proceedings have been undertaken, elements of the file relating to the identity of the issuer and the targeted persons are destroyed within two months from the closure of the operations of admissibility and verification.

- When disciplinary or judicial proceedings have been undertaken, elements of the file are retained for a period not exceeding the litigation timeframe.

In any event, for the purposes of traceability and reporting, the name of the entity concerned and the date of the alert, with a short description of the facts, may be retained, excluding any information relating to the identity of the persons concerned.



## 10. How is the issuer protected?

► If the facts reported prove to be incorrect, no action will be taken against the alert issuer, as long as the latter acted in good faith. Here, bad faith means knowledge of the falsity of the allegations.

Disciplinary sanctions and, where appropriate, judicial proceedings may be taken against an alert issuer acting in bad faith. This will notably be true in the case of malicious, vexatious or defamatory allegations or a wrongful alert.

If disciplinary proceedings are to be brought against the issuer, and consequently their identity is to be disclosed, they will be informed prior to the initiation of proceedings.

Any alert issuer who acted in good faith is protected by Saint-Gobain as follows:

- No sanctions
- No legal proceedings
- No retaliation

The issuer may also benefit from reinforced legal protection. For more information, see [next page](#).





**Several legislations** grant special protection to certain kinds of alert issuer or whistle-blower.

The French “Sapin II” Act, for example, has created a specific status for natural persons issuing alerts. Obtaining this protected status is subject to the following three conditions:

1. Reporting a serious breach that would constitute:
  - a crime or an offence;
  - a serious and manifest breach of the law or a regulation;
  - a serious and manifest breach of an international undertaking regularly ratified or approved by France, or of a unilateral act of an international organization taken on the basis of such an undertaking;
  - a threat or serious damage to the general interest.
2. Having personal knowledge of the facts reported.
3. Acting selflessly and in good faith.

A whistle-blower within the meaning of this law:

- Is not criminally liable, on condition that the disclosure of the information is necessary and proportionate to the safeguarding of the interests in question, and done in accordance with the procedures for reporting alerts.
- Cannot be dismissed, sanctioned or discriminated in any way for reporting facts in accordance with the procedure for reporting alerts.

**Other countries** also grant conditional protection to whistle-blowers. For more information, contact your local legal team.



I am

- a Saint-Gobain personnel
- an external employee
- a supplier

And I want to report a serious breach



I alert!

- I alert by email or by mail
- I provide the documents/information in my possession by completing a questionnaire

It is confidential and I am protected



- Reinforced legal protection for certain alert issuers depending on their countries
- Saint-Gobain commitments for any alert issued in good faith:
  - No sanctions
  - No legal proceedings
  - No retaliation

Many teams are on hand to answer your questions or to give you more information on the Saint-Gobain Group’s alert system.

**Group**  
Group General Secretary  
Compliance team at the Compagnie de Saint-Gobain

**Delegation**  
Legal departments of Delegations

**Sector**  
Legal departements of Sectors

The list of persons to contact is appended to this Guide.

[Resource 1:](#) Current list of email boxes inside the Saint-Gobain Group

[Resource 2:](#) Officers’ charter

[Resource 3:](#) Who to contact

