ETHICS & COMPLIANCE BY SAINT-GOBAIN

ETHICS AND COMPLIANCE DEPARTMENT

POLICY ON THE GROUP ALERT SYSTEM

ORGANIZATION AND GROUP PROCEDURES

11/2020

SAINT-GOBAIN

Summary

"At Saint-Gobain, we are deeply committed to our values. When you speak up, you help us living up to them and building our common culture together. As early as 2011, the Saint-Gobain Group set up an ethics and professional alert system. This system, open to all of the Group's stakeholders (customers, suppliers, shareholders, trade unions, NGOs, local communities or authorities, the State, etc.) allows everyone to report, if they wish to do so and in complete confidentiality, breaches of the law, our Principles of Conduct and Action and our internal policies.

Available online, operated with discretion, professionalism and impartiality, this system protects our employees, our stakeholders and the Group itself. It is also a powerful driver of our organization's continuous evolution.

We are here to listen, ready to act responsibly and transparently.

Feel free to speak up!"

Benoit Bazin,
Saint-Gobain Chief Executive Officer

The ethics and professional alert system (or "**alert system**") is the cornerstone of the measures implemented by Saint-Gobain to protect its employees, stakeholders and the Group itself, and to identify areas in which the organization can evolve or improve.

To be effective, the alert system must be broadly known and fully understood by all its users. This Policy thus explains the framework of the system, its main features and the rights and obligations of the persons concerned. It is broadly disseminated.

This Policy is anchored in Saint-Gobain Group's Principles of Conduct and Action, specifically the principles of Respect for Others and Respect for the Law.

It also meets the Group's **international commitments**, which include:

- the United Nations Charter of Human Rights;
- the United Nations Convention against Corruption;
- the ten principles of the Global Compact; and
- the Organization for Economic Co-operation and Development ('**OECD'**) Guidelines for Multinational Enterprises.

As Saint-Gobain is a French group, this Policy complies with the requirements set out by **French law**, which all Group entities and subsidiaries must comply with, regardless of where they are established or operate from. These include:

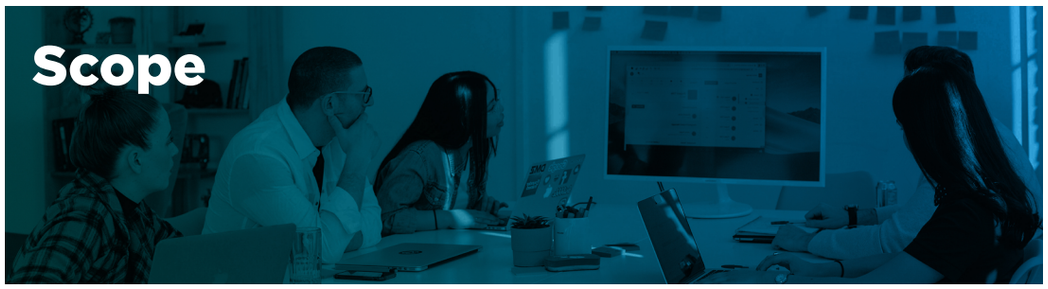
- The so-called «Sapin II» law[1], including the provisions regarding the protection of whistleblowers (art. 6-16) and those relating to measures to fight corruption (art. 17);
- The law on the duty of vigilance[2];
- The EU Directive on the protection of whistleblowers[3] (to be transposed into Member States' respective legislations); and
- General legislative measures for the protection of individuals (including provisions on sexual and moral harassment, as well as all forms of discrimination).

[1] Law No. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernization of economic life, and its implementing Decree No. 2017-564 of 19 April 2017. This Policy amounts to an 'internal procedure' within the meaning of the decree. It is also mentioned in the Group Anticorruption Policy, to which it is incorporated by reference.

[2] Law no. 2017-399 of 27 March 2017 relating to the duty of vigilance of parent and subcontracting parties.

[3] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

Finally, this Policy complies – both in its principles and spirit – with **non-French laws** which apply to the Group's subsidiaries. Should the requirements of these laws not be aligned with this Policy, the latter will be adapted locally, while seeking always to apply the Principles of Conduct and Action and the Group's international commitments in the area of whistleblowing as extensively as possible.



The entire Group is subject to the requirements of this Policy. The Saint-Gobain Group ("**Saint-Gobain**" or the "**Group**") means, collectively, Compagnie de Saint-Gobain and all the companies it controls[4], whether exclusively or jointly. In joint-ventures which Saint-Gobain does not control, in the absence of an equivalent alert system policy, the Group's representatives must ask the competent corporate bodies to adopt and deploy this Policy.

All alerts, issued and treated within the framework of this Policy, are subject to the full provisions of this Policy.

[4] The term control refers to the ownership or holding, directly or indirectly, of more than 50% of the voting rights of a company and/or the power, in fact or in law, to direct or appoint the management of a company.

Who can issue an alert?

Persons who can issue an alert are:

- The Group's internal, external or occasional **employees** (fixed-term or permanent employees, apprentices, trainees, temporary workers, as well as employees of subcontractors or consultants present on site);
- The Group's "**stakeholders**", i.e. third parties having an interest in the Group's activities because:
  * They take part in its economic life (customers, suppliers, shareholders);
  * They observe or influence the Group's behavior both internally and externally (trade unions, NGOs); or
  * They are affected, directly or indirectly, by its activities (communities or local authorities, State…) in a positive or negative way.

On what grounds can an alert be issued?

Subject to the conditions of admissibility, an alert may concern:

- Any conduct or situation contrary to the Group's Anticorruption Policy;
- Failure to comply with the Principles of Conduct and Action;
- A crime or misdemeanor;
- A clear and serious breach of:
  * an international commitment ratified or approved by France;
  * a unilateral act of an international organization taken on the basis of such a commitment; or
  * the law or a regulation;
- A threat or serious prejudice to the general interest;
- A serious harm[5] to:
  * human rights;
  * the health and safety of persons; or
  * the environment.

[5] Such harm resulting from the Group's activity or that of its subcontractors or tier-one suppliers (when this activity is within the framework of the contractual relationship with the Group).

Concretely and to illustrate, such issues may arise in the following areas:

- the Principles of Conduct and Action;
- corruption and influence peddling;
- anti-competitive practices;
- freedom of association, the use of forced labor and child labor – issues addressed in the Group Policy on Human Rights;
- employee rights, such as no discrimination, moral or sexual harassment;
- theft, money laundering, embezzlement and fraud (including financial, accounting, tax and banking matters);
- export controls, economic sanctions and embargoes;
- environmental protection; or
- health and safety at work.

This list is not exhaustive and these areas are likely to evolve over time.

Several reporting channels are available to report an incident.

The Group online alert system (BKMS® System)

Saint-Gobain Group's online alert system (BKMS® System) is an online platform developed by an external service provider, Business Keeper AG. It is operated by Saint-Gobain.

This system is highly secure: neither the service provider nor any third party[6] has access to the data contained in the system.

Received by the Ethics and Compliance Department, alerts are treated by the persons specifically authorized to do so under this Policy: Alert Examiners.

[6] Subject, as the case may be, to a court order (or other legally binding decision) requiring the Group to provide the information.

This system is open to all employees (internal, external or occasional) as well as stakeholders. Available in many languages, it allows the collection of alerts, whether anonymous or not. The practical details of its use are explained on the intranet, as well as on the Group's websites. It can be accessed via the following url:

https://www.bkms-system.net/saint-gobain

NB. Some countries have set up automated alert systems separate from the Group's online alert system, which operate according to these countries' specifications and are available on their respective local intranets. When these systems are needed to meet specific regulatory requirements, they may continue to coexist with the Group's system. If not, it is intended that they will give way to the Group system.

Mail

Alerts can also be submitted via postal mail. In this case, it is preferable to send the letter by registered mail with acknowledgement of receipt. This precaution will secure the collection of the alert and allow the date of the alert to be established with certainty.

Furthermore, to ensure the confidentiality of the alert, it is recommended to use a double envelope system. The inner envelope should be marked "REPORTING AN ALERT" and the date the letter is sent. The outer envelope should display the following address:

Compagnie de Saint-Gobain
Ethics and Compliance Department – CONFIDENTIAL
Tour Saint-Gobain
12, place de l'Iris
92400 Courbevoie
France

This channel is available to all employees (internal, external or occasional) as well as stakeholders and allows the collection of alerts, anonymous or not.

In some countries, a local address is also available. The list of such addresses is available on the intranet, as well as on the website of the relevant country.

Phone

In some countries, a telephone number is made available for people wishing to report an incident. This channel is available to all employees (internal, external and occasional) as well as to stakeholders, as the case may be. It allows the collection of alerts, whether anonymous or not.

The local phone numbers as well as the instructions for issuing an alert via such channel are available on the intranet and on the website of such relevant countries.

Via an Alert Examiner

It is also possible for employees (internal, external and occasional) to make an appointment with an Alert Examiner (in person, by phone or digitally) in order to report an incident directly. The list of Alert Examiners is available on the intranet.

Use and choice of channel at reporter's discretion

The use of the above-mentioned channels is optional and the choice of channel is free.

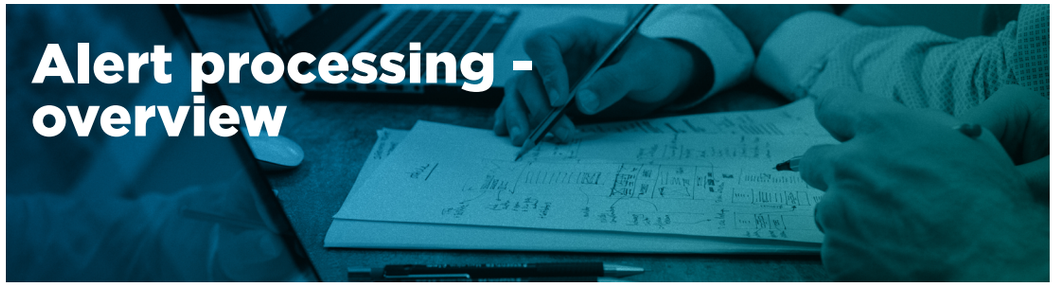
Employees may of course contact their managers, human resources managers, in-house lawyers or employee representative bodies.

The alert channels described in this Policy are complementary and alternative means of reporting, when the "usual" communication or reporting modes are unavailable or unpractical, turn out to be ineffective, or generate anxiety for the reporter (e.g. a request has gone unanswered, or the person subject of the complaint is the reporter's line manager).

May an alert be issued anonymously?

Most of the available reporting channels allow you to send an alert anonymously. This possibility is part of the Group's intention to allow broad and uninhibited access to the alert system.

However, the Group encourages reporters to identify themselves. Indeed, an alert which is not anonymous will in fact be handled more efficiently.



Alert processing - overview

Once an incident has been reported, the relevant Alert Examiner verifies the **alert's admissibility**, i.e. that it falls within the scope of this Policy. He informs the reporter that his rights, as set out in this Policy and guaranteed by law (including full **whistleblower protection** as the case may be) will be protected.

The **Alert Examiner** then conducts an **investigation** to determine whether the **facts** are established and the **conclusions** to be drawn.

The Alert Examiner sets out his recommendations, which are taken into account by the **management** in charge of making a **decision** for the persons and/or the department concerned. In the event of management's failure to act or diverging views with the Alert Examiner, the case is presented to the **Group's Ethics Committee**.

Who receives and processes alerts?

From the receipt of an report to the submission of recommendations to the management, alerts are handled by the Alert Examiners, who discharge their duties under the supervision of the Ethics and Compliance Department.

Who are the Alert Examiners?

Alert Examiners are Group employees specially authorized to receive and process alerts. In the performance of their duties, they report to the Chief Ethics and Compliance Officer who carries out his/her mission under the General Secretary's supervision.

They have the necessary skills, authority and resources to discharge their duties in a confidential, professional and impartial manner within the framework of this Policy.

Specifically, the network of Alert Examiners is composed of:

- **At central level:**
  - The Chief Ethics and Compliance Officer;
  - The Group Fraud Officer; and
  - The Group HR Alert Examiner for alerts predominantly related to human resources.
- **In the countries:**
  - The Ethics and Compliance Officer; and
  - If necessary, HR Alert Examiner(s), appointed by the country's HR Director from the human resources department for alerts predominantly related to human resources.

The names and contact details of the Alert Examiners are available on the intranet. Depending on the specific needs of an investigation, they may designate one or more *ad hoc* Alert Examiners, who are bound by the same obligations as the Alert Examiners themselves. They may also, when justified under the circumstances, delegate investigations to specialized external professionals who are bound – by contract or by

law – to an obligation of confidentiality. By signing the **Alert Examiner Charter**, each Alert Examiner personally undertakes to respect the following obligations:

- Obligation of **strict confidentiality** applicable in all alert procedures, protecting the identity of the whistleblower (when he is not anonymous); the identity of the persons mentioned in the alert or subject of the complaint; and all information collected during processing of the alert. This information (with the exception of the identity of the whistleblower as such) may, however, be communicated in a restricted and limited manner for the purposes of the investigation.
- Duty of **impartiality**: the Alert Examiner acts professionally, without prejudice and represents no particular interests when carrying out his mission.
- Obligation of **transparency and loyalty** towards the persons whose data is processed as part of the alert treatment: the Alert Examiner informs, pursuant to the terms of this Policy, the whistleblower and the persons mentioned in the alert or subject of the complaint.

The Ethics and Compliance Department ensures strict compliance with the above principles by all Alert Examiners.

Which Alert Examiner receives and processes the alert?

Alerts are received by the Ethics and Compliance Department, which redirects them so that they can be dealt with by the most appropriate members of the Alert Examiners network.
As a general rule, alerts are processed by the Alert Examiner of the country concerned by the alert. Alerts may however be transferred so as to be dealt with centrally, either at the request of the local Alert Examiner or at the discretion of the Ethics and Compliance Department at Group level.

Notwithstanding the above, the following alerts are treated centrally at Group-level (unless they are referred locally at the discretion of the Ethics and Compliance Department):

- Alerts concerning:
  - a real or suspected case of corruption or influence peddling;
  - an actual or alleged violation of competition law;
  - an actual or alleged violation of economic sanctions or export control regulations;

- Alerts involving one or more members of management in a country;
- Alerts that may lead to a significant overall financial risk; and
- Alerts where a particular circumstance (e.g. a conflict of interests) prevents the case from being treated locally in a serene and impartial manner.

The Alert Examiner who is seized first decides on the alert's admissibility. Only admissible alerts are investigated.

An alert is admissible when:

1. It is issued on one of the **grounds set out** in this Policy[7];
2. The reporter acts in **good faith**[8] and in a **disinterested** manner; and
3. The alert concerns facts of which the reporter has **personal knowledge** (direct witness or even victim).

The Alert Examiner determines if the alert is admissible. If he is not in a position to make a decision, he may request additional information from the reporter (unless he has no means of contacting him). Within a reasonable timeframe, he informs the reporter whether the alert is admissible or not.

The Alert Examiner also reminds the reporter that he benefits from the "whistleblower" protection described in this Policy, provided of course that the investigation does not subsequently reveal grounds for exclusion (e.g. lack of good faith) that could lead to possible disciplinary measures or even legal proceedings against the reporter.

[7] See ON WHAT GROUNDS CAN AN ALERT BE ISSUED?

[8] A person is considered to be acting in bad faith if he/she denounces facts that he/she knows to be false, or with the intention of causing harm, or in the hope of obtaining an undue advantage, or if he/she knowingly makes vexatious or defamatory allegations against a third party.

The purpose of the treatment is to establish whether the facts set out in the alert are true and to determine the conclusions to be drawn.

Processing an alert is made easier if the facts are described in an objective and detailed manner (e.g. dates, entity and persons concerned), and if the reporter provides, if possible, information or documents (under any form and medium) likely to substantiate the alert.

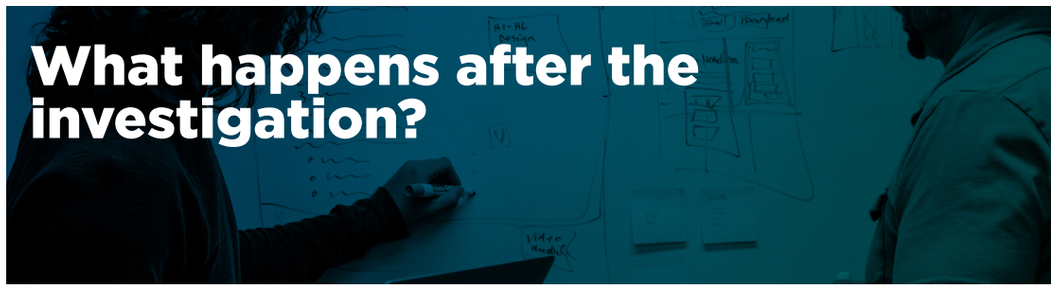
Admissible alerts are dealt with according to the guidelines set out below[9]:

- The Alert Examiner (or, when justified by the circumstances, an external professional) diligently investigates the facts reported in the alert. To this end, the Alert Examiner has the power, in the performance of his/her duties, to consult internal documents and to solicit persons likely to shed light on the facts. He applies a principle of relevance and minimization of the data collected and processed, including by informing the solicited persons of the confidential nature of the investigation.
- Depending on the nature and seriousness of the facts, the Referent may be assisted in the investigation by Group employees and/or external experts. Their number is limited to the strict minimum. They receive the information required to deal with the alert, in accordance with their respective responsibilities. Beforehand, they are informed of the confidential nature of the information provided, and sign a strict confidentiality agreement similar to the Alert Examiner Charter.
- Upon receipt of the alert, the Alert Examiner determines whether measures need to be taken to ensure the protection of persons and property and the preservation of evidence. Such measures may justify postponing the time when the persons mentioned in the alert or subject of the complaint are informed.

[9] With the exception, where applicable, of alerts received via dedicated national systems.

When the Alert Examiner considers he has gathered enough to conclude the investigation, he closes it and communicates his conclusions to the appropriate management. In this respect, he may:

1. Recommend that the alert be dismissed if the facts are not established or do not require further action; or
2. Issue recommendations regarding the alert follow-up.



What happens after the investigation?

The appropriate management decides on the follow-up to be given to the alert, taking into account the conclusions of the Alert Examiner. Such follow-up may include an action plan (service reorganization, training), disciplinary sanctions or even legal proceedings.

If the management does not follow the Alert Examiner's conclusions, the case is presented to the Group Ethics Committee, composed of the Group's General Secretary, the Senior Vice-President – Human Resources, and the most senior manager of the region or activity concerned. The Chief Ethics and Compliance Officer takes part in the discussions, but has no vote in the Committee's deliberations.

What information after the alert?

Once the management (or the Ethics Committee, as the case may be) has made a decision regarding the alert, the Alert Examiner keeps the reporter informed of the outcome of the alert.

How are the rights of individuals protected?

In all cases, users of the alert system are invited to consult the detailed information notice relating to the processing of personal data which is made in the context of the alert system (the "**Information Notice**").

General principle of confidentiality

The principle of confidentiality is the bedrock of individuals' rights protection within the framework of the alert system. Confidentiality is embedded in the system in several ways:

- The Alert Examiners, acting under the supervision of the Ethics and Compliance Department, make a personal commitment by signing the Alert Examiner Charter;
- Information is collected and processed according to a principle of relevance and minimization; and
- The Group undertakes to protect the confidentiality of the personal data of the concerned parties (i.e. the whistleblower and the persons mentioned in the alert or subject of the complaint), in accordance with the terms of this Policy.

Please note that the Sapin II law has introduced an offence[10] sanctioned by 2 years of imprisonment and a fine of 30,000 euros (150,000 euros for legal persons) for breaching confidentiality regarding the identity of the whistleblower, the persons subject of the complaint, and all the information collected in the course of processing the alert.

This obligation applies to everyone, including the whistleblower whose alert must mandatorily follow the three successive steps as provided by law[11] :

1. the report is made through the internal channels described in this Policy (line manager, online system, mail, etc.). This step enables the company to solve the issue, as the case may be, and to take all adequate measures to prevent similar events from occurring in the future;

[10] Article 9, Law n° 2016-1691 of 9 December 2016 relating to transparency, the fight against corruption and the modernization of economic life.

[11] Article 8, Law n° 2016-1691 of 9 December 2016 relating to transparency, the fight against corruption and the modernization of economic life (Sapin II).

2. if the recipient of the alert does not take steps to check its admissibility within a reasonable time, the whistleblower may report to the judicial authority, administrative authority or professional bodies; and
3. as a last resort, if the competent authorities mentioned in step 2 fail to handle the alert within three months, the alert may be made public.

Failure to proceed as per the above order will result in the reporter not being entitled to the protections set out in this Policy. However, the first step is not necessary in the event of serious and imminent danger or in the presence of a risk of irreversible damages.

Protection of the whistleblower

Notwithstanding other protections the whistleblower may benefit from under the regulations applicable to him, the Group undertakes through this Policy to provide the following protections to the reporter of an admissible alert:

- Saint-Gobain will not take any disciplinary action, legal proceedings or any other retaliatory measure against the whistleblower on the grounds he would have issued an admissible alert (this even if the facts – reported in good faith – turned out to be false, or if the alert is closed without further action)[12] ;
- the whistleblower will be informed of his/her rights, in particular those resulting from the applicable regulations on the protection of personal data, as detailed in the Information Notice[13] ; and
- information likely to identify the whistleblower (if known) may only be disclosed with his consent (except to a competent judicial or administrative authority).

[12] By extension, no sanctions or reprisals will be taken against colleagues or any person who assisted the whistleblower to make the report (a "facilitator"), or against the company that employs the whistleblower if he is an employee or associate of a third party company (client, service provider, etc.).

[13] The Information Notice explains how the rights relating to the protection of personal data can be exercised.

Warning

Abuse. The abusive use of the alert system may, in any event, expose the perpetrator to disciplinary sanctions and, where appropriate, legal proceedings.

Self-incrimination. If the reporter has taken part in the unlawful act he reports in the alert, he is nonetheless liable to disciplinary sanctions or even prosecution for the act in question. Nonetheless, the Group will take into consideration the genuine and transparent nature of the report.

Professional secrecy. The whistleblower cannot be prosecuted for breach of professional secrecy if the information he reveals or reports is covered by it. However, such immunity does not cover facts, information or documents (regardless of their form or medium), which are covered by the national defense secrecy, medical secrecy or legal privilege.

Rights of persons mentioned in the alert or subject of the complaint

Notwithstanding other protections they may benefit from under the regulations applicable to them, the Group undertakes through this Policy to provide the following protections to the persons mentioned or subject of the complaint:

- they will be informed in accordance with applicable regulations regarding the protection of personal data, as detailed in the Information Notice ; and
- the confidentiality of their identity will be particularly preserved throughout the treatment of the alert, and their presumption of innocence will be strictly respected.

[14] See Article 122-9 of the French Criminal Code.

[15] The Information Notice explains how the rights relating to the protection of personal data can be exercised.

The personal data processed in the context of an alert are subject to an archiving policy detailed in the Information Notice.

Good knowledge and understanding of this Policy is essential to its effectiveness: it is widely disseminated by all means, including digital or face-to-face presentations and poster campaigns.

Compliance with this Policy is a matter concerning all employees, regardless of their tasks and level of responsibility. Managers play a fundamental role in developing, disseminating and upholding the Group's compliance culture.

This Policy is under the responsibility of the Ethics and Compliance Department, which is in charge of periodically updating it – in particular to reflect changes in the law – ensuring its deployment and monitoring, and reporting on its implementation to the Group's governing bodies.

01 ORGANIZATION AND GROUP PROCEDURES

11/2020

SAINT-GOBAIN

ETHICS & COMPLIANCE
BY SAINT-GOBAIN