
SII ALERT SYSTEM USER GUIDE

Version 04

Reference Date: **December 2025**

Document created from **S4-0072-23** standard.

SII Internal Validation			
	Last Name / First Name	Function	Date
Writing	Romain Le Besnerais	Internal Audit	December 2025
Verification	Bénédicte Querenet-Hahn	External member of SII Ethics Committee	December 2025
Approval	Eric Matteucci	Chairman of the Board	December 2025

Distribution List		
Company	Department/Service	Last Name / First Name
SII	All Employees	

Version Log		
Date	Version	Version Purpose
December 2020	01	Creation
January 2023	02	Update
July 2024	03	Review
December 2025	04	Update

Table of Contents

1. Context and objectives of the SII alert system	5
2. Preliminary definitions	5
3. The different reporting channels	7
3.1. Internal channel	7
3.1.1. Written or oral reporting	7
3.1.2. Reporting via the SII Integrity Line platform	7
3.1.3. Assignment of received reports	8
3.1.3.1. Reports received outside the platform by a member of a Local Ethics Committee	8
3.1.3.2. Reports received outside or via the SII platform by the SII Ethics Committee	8
3.2. The external channel	9
3.3. Public disclosure	9
4. The platform's scope of application	10
4.1. Conditions related to the whistle-blower	10
4.2. Conditions related to the object of the Report	10
5. How the system works	11
5.1. Optional use of the System	11
5.2. Protection of the whistle-blower and his/her entourage against retaliation	11
5.3. Identification of the Reporting Person - Anonymity	11
5.4. Confidentiality	12
5.5. Presumption of Innocence	12
6. Reporting and handling of reports	12
6.1. Receipt of the Report	12
6.2. Assessment and processing of the report	13
6.3. Information of the Persons Concerned and Third Parties Mentioned in the Report: ...	14
7. Protecting the personal data collected and processed under the system	15
7.1. Data processed on the Platform	15
7.2. Purposes of processing Personal Data	15
7.3. Recipients of Personal Data collected and processed on the Platform	15
7.4. Alert Register	16
7.5. Duration of retention of Personal Data	16



7.6. Security and Privacy 16

7.7. Rights relating to personal data 17

8. Miscellaneous 18

8.1. General Policy 18

8.2. Effective Date and Amendment of the Guide 18

8.3. Updates 18

9. Information and contact persons..... 18

1. CONTEXT AND OBJECTIVES OF THE SII ALERT SYSTEM

Development and business conduct within SII is based on principles of integrity, exemplary behaviour, and transparency. SII's ethical policy formalizes these commitments that must guide the actions of everyone, regardless of geographical or cultural context, the status or position within the organization.

SII provides an internal Whistle-blower Alert System to all "Interested Persons" for reporting any violation or attempted concealment of a violation of law or regulation, or conduct contrary to the Internal Regulations, the Ethics Charter, the Code of Conduct or the Anti-Corruption Code of Conduct as well as any other internal rules of SII or a threat or harm to the general interest in order to take appropriate corrective measures.

In setting up the System, SII has ensured that it is designed, developed and implemented so as to preserve the identity of the whistle-blower, the persons concerned in the alert, the mentioned third parties and to keep the facts reported confidential.

The System is implemented and monitored by the Head of Internal Audit as well as by the members of the SII Ethics Committee and Local Ethics Committees.

The purpose of this guide (the "Guide") is to detail the procedures for implementing and using the System.

2. PRELIMINARY DEFINITIONS

- **Alert** refers to a report made in good faith and without direct financial compensation.
- **Reporting Person** or **whistle-blower** refers to the person who makes a report.
- **Post Box** refers to the access to the SII Integrity Line that is automatically created when a Report or question is sent. This Post Box allows the whistle-blower to exchange with the Ethics Committee in charge of processing the Report or question.
- **Employee** refers to SII's employee, occasional or external collaborator, or executive officer.
- The **SII Ethics Committee** refers to the Ethics Committee of SII France. This SII Ethics Committee has three members, one of whom is external and independent.
- The **Local Ethics Committee** refers to the Ethics Committee of the SII subsidiary or controlled company in charge of the Report.
- **Platform** refers to the system for collecting and processing reports which allows any Interested Person to make a report.

- **Personal Data** refers to the following categories of personal data that may be processed within the Platform:
 - the identity, functions and contact details of the whistle-blower;
 - the identity, functions and contact details of the persons mentioned in the Alert and any third party mentioned in the Report;
 - the identity, functions and contact details of persons involved in collecting or processing the Report;
 - the facts, information and documents collected in the context of receiving and processing the Report;
 - the report of verifications and the outcome of the Report;
 - the follow-up to the Report.
- **Facilitator** refers to any natural or legal person who is a non-profit private entity that assists a whistle-blower in making a report or a public disclosure.
- **Whistle-blower** refers to a person who, in good faith and without direct financial compensation, reports or discloses information concerning a crime or offense, a threat or harm to the public interest, a violation or attempted concealment of a violation of an international commitment duly ratified or approved by France, of a unilateral act of an international organization based on such a commitment, of European Union law, of national law or regulations, or of behaviour contrary to the Internal Regulations, Ethics Charter, Code of Conduct and Anti-Corruption Code of Conduct as well as any other internal rules of SII.
- **Data Subject** refers to any person whose Personal Data is processed within the Platform (for example, the whistle-blower, a Person under Investigation, a person heard as part of the investigation, etc.).
- **Authorized Persons** refers to the Head of Internal Audit and members of the SII Ethics Committee or, as the case may be, members of the Local Ethics Committee. They may also involve other persons to assist with the collection, processing, and resolution of the Alert, such as officers, employees or external advisors (lawyers and accountants).
- **Interested Person** refers to any individual associated with SII such as SII employees and contractors, shareholders or partners of SII and its subcontractors, member of the management, administrative or supervisory bodies of SII and its subcontractors, former employee or job applicant, as well as any occasional and external collaborator of SII and any person who has the right to report an alert.
- **Person Concerned** means a natural person (or legal entity) who is mentioned in the Report as the person to whom the violation is attributed or to which that person is associated.
- **SII Integrity Line** refers to the external secure online platform that allows SII Employees and external Stakeholders to issue Reports and/or ask questions of the Ethics Committee.
- **SII** refers to SII France and its subsidiaries and controlled companies.

- **Report** refers to any information that concerns SII or any related person reported or disclosed by an Interested Person, concerning a crime, offense, threat or harm to the public interest, a violation or an attempt to conceal a violation of the law or regulations, or behaviour that is contrary to the Internal Regulations, the Ethical Charter, the Code of Conduct, the Anti-Corruption Code of Conduct and other internal rules of SII. However, facts, information or documents whatever their form or medium that are covered by national security secrecy, doctor-patient confidentiality or attorney-client privilege may not be reported under the System.

3. THE DIFFERENT REPORTING CHANNELS

The whistle-blower has the choice of 3 channels to make their report.

3.1. Internal channel

3.1.1. Written or oral reporting

Any person who has a concern can report it in writing or verbally to a member of the SII Ethics Committee or the Local Ethics Committee. If the report is addressed to someone else, that person must immediately transmit it to a member of the SII Ethics Committee or the Local Ethics Committee of the entity concerned.

The member who receives the report will enter it into the SII Integrity Line platform (see §3.1.2) to facilitate the processing.

If the whistle-blower wants to make an oral report, they can do so over the phone or request a video or in-person meeting. If a meeting is requested it must be organized no later than twenty working days after the receipt of the request. If the whistle-blower consents, the member of the Ethics Committee who receives it will record the oral report in writing. The whistle-blower has the right to verify, correct and approve the report by signing it. The report is then entered into the SII Integrity Line platform (see §3.1.2) to facilitate its processing. The whistle-blower receives a reference number and password for accessing the platform so that they can exchange information confidentially and securely with the Ethics Committee in charge of processing their report.

3.1.2. Reporting via the SII Integrity Line platform

An interested person has the option to report an incident directly to the SII Ethics Committee via the secure external platform called SII Integrity which is accessible online at:

<https://sii.integrityline.fr/>

SII Integrity Line is a computer system developed by an external provider, EQS Group. It is available in French, English, Spanish and Polish throughout the year. The whistle-blower can keep track of their Report by logging in with the reference number assigned to them upon submission and the password they created. The whistle-blower then follows the process suggested by the platform to submit their report, which can be anonymous if preferred. Upon submission, a secure and personal Post Box is automatically created for the whistle-blower to receive updates and information on their report's progress. The Post Box also allows for communication between the author and the Ethics Committee members responsible for processing their report. The whistle-blower can provide supporting documents, photos or any other necessary information at any time. More information on the terms of use and confidentiality of communication via the platform is available in the FAQ section (<https://sii.integrityline.fr/>).

It is important to note that the Ethics Committee may investigate any reports submitted and the steps for the investigation are explained below.

3.1.3. Assignment of received reports

3.1.3.1. Reports received outside the platform by a member of a Local Ethics Committee

Reports received outside the platform by a member of a Local Ethics Committee are processed by this Committee, unless its members believe that they cannot independently and impartially process the facts, for example because the report concerns the Country Director of the local entity.

In such a case, the Local Ethics Committee immediately informs the whistle-blower of its inability to process their report and invites the whistle-blower to withdraw it and submit it to the SII Ethics Committee via the platform so that the latter can process it.

3.1.3.2. Reports received outside or via the SII platform by the SII Ethics Committee

Reports received by any member of the SII Ethics Committee, whether outside or through the SII Integrity Line platform are processed by the SII Ethics Committee. If a report received by the SII Ethics Committee targets one of its internal members, the external member will immediately withdraw the access rights of both internal members to the report and will process the report independently and impartially.

If the SII Ethics Committee believes that the Local Ethics Committee of a subsidiary or controlled company would be more effective in handling a particular report, the SII Ethics Committee may delegate some or all of the processing responsibilities to the Local Ethics Committee.

3.2. The external channel

The whistle-blower can make a report either internally first or directly:

- to the competent external authorities as defined in the appendix of decree n° 2022-1284 implementing the law on whistle-blower protection of October 3, 2022: <https://www.legifrance.gouv.fr/loda/id/LEGISCTA000046357770>;
- to the judicial authority;
- to the Defender of Rights;
- to the competent EU institutions, bodies or organizations.

3.3. Public disclosure

It is important to note that the whistle-blower can only publicly disclose their report if:

- after the whistle-blower has previously made an external report, with or without an internal report, no appropriate action has been taken in response to it within a reasonable period of time not exceeding three months from the acknowledgment of the report or, failing that, three months from the end of a period of seven working days following the report;
- there is a serious and imminent danger, especially in situations of emergency or risk of irreversible harm;
- the use of the external channel would expose the whistle-blower to a risk of retaliation or would not allow for an effective remedy of the subject of the disclosure, due to the specific circumstances of the case, particularly if evidence can be concealed or destroyed, or if the whistle-blower has serious reasons to believe that the authority may be in a conflict of interest, collusion with the perpetrator, or involved in the reported wrongdoing.

4. THE PLATFORM'S SCOPE OF APPLICATION

A report submitted by any Interested Person falls within the scope of the Platform, under the conditions specified below:

4.1. Conditions related to the whistle-blower

Only Interested Persons are allowed to submit a report on the Platform.

The whistle-blower may report facts that have been reported to them in the professional context, even if they have not personally witnessed them. However, the whistle-blower is not authorized to report on incidents that they have not personally witnessed, except within a professional context.

Only reports relating to a crime, offense, threat or harm to the public interest, a violation or attempted concealment of a violation of the law or regulation, or conduct contrary to the Internal Rules, the Ethical Charter, the Code of Conduct, the Anti-Corruption Code of Conduct, and other internal rules of SII may be collected on the platform.

4.2. Conditions related to the object of the Report

In order for it to be considered and processed, any report must contain specific elements including:

- the country and nature of the reported facts and information;
- the identity, function, and country of origin of the whistle-blower and the entity in which the whistle-blower carries out their functions unless they have chosen to remain anonymous;
- the identity, function, and entity of the targeted person(s) and third parties mentioned in the report;
- the most precise and objective description possible of the reported facts (factual description, date, location, entity concerned).

The elements provided in the report must be directly related to the scope of the system and strictly necessary for the verification of the reported facts. The statements used to describe the reported facts must indicate their alleged nature. If the whistle-blower is uncertain about the facts they are reporting they must clearly state so.

Authorized Persons are available to any interested person for any questions regarding the application or interpretation of this Guide.

5. HOW THE SYSTEM WORKS

5.1. Optional use of the System

The use of the Platform is optional. No sanction will be imposed on any person for not using this System.

5.2. Protection of the whistle-blower and his/her entourage against retaliation

If any interested person uses the Platform in good faith and without any direct financial reward to report facts that fall within the scope of the Platform, they cannot be subject to direct or indirect retaliation, even if the reported facts later prove to be inaccurate or do not result in any action.

This protection also applies to Facilitators and natural persons linked to the whistle-blower (such as colleagues and close associates), as well as to legal entities/juridical entities controlled by the whistle-blower, for whom he/she works or with whom he/she is in a business relationship.

Any person who believes that he/she is the subject of retaliation is invited to report it to the SII Ethics Committee by email at the following address:

comite-ethique-siigroup@sii.integrityline.org

On the other hand, the abusive use of the System, including the reporting of allegations that the Interested Person knows to be false, may result in disciplinary sanctions or even legal action.

5.3. Identification of the Reporting Person - Anonymity

To ensure the report is handled effectively, it is recommended that the whistle-blower reveals their identity.

Nevertheless, it is possible to make a report anonymously. Interested Persons should be aware that anonymous reports should not be privileged since:

- their verification is more complex when their author remains anonymous
- the Person Concerned by the report may discover the identity of the whistle-blower by other means.
- SII cannot supervise the protection of the whistle-blower if he/she remains anonymous.

5.4. Confidentiality

The Platform has been designed to ensure that the identity of the whistle-blower, the Person Concerned, and any third parties mentioned, as well as the information subject to the Report, are kept strictly confidential at all stages of the receipt, examination, and processing of the Report. However, SII would like to remind all that the authorities may request the identity of the whistle-blower, Concerned Person, third parties mentioned, and reported facts, even if they were kept confidential.

5.5. Presumption of Innocence

Any person who is the subject of a report is presumed innocent until the allegations against them are proven.

6. REPORTING AND HANDLING OF REPORTS

The processing steps of the report are described below.

6.1. Receipt of the Report

Upon receipt of any report, the Local Ethics Committee or the SII Ethics Committee, depending on who received it will:

- Inform the whistle-blower of the receipt of their report and the processing of their personal data within 7 working days of receipt of the report.
- Direct, if necessary, the Whistle-blower to the appropriate person, for example if the report does not fall within the scope of the Platform.
- Invite the whistle-blower to identify themselves, indicate their position, and provide their contact details.
- Request from the whistle-blower to provide necessary information for the processing of their report, in particular:
 - the identity and functions of the Concerned Person targeted and third parties mentioned in the report
 - the facts, information and documents to support the report
- Invite the whistle-blower to only provide relevant and necessary information related to the reported facts.

If the whistle-blower wishes to remain anonymous, the member of the relevant Ethics Committee informs them that:

- the investigation may be more difficult to conduct.
- SII cannot provide protection to the whistle-blower if they remain anonymous.
- the Concerned Person targeted by the report may still discover the identity of the Author through other means.

They also inform the whistle-blower of:

- the functioning of the Platform
- the guarantees they benefit from, in particular their protection status
- the risks they run in case of abusive use of the Platform (disciplinary sanctions or even legal action)

When the report has been made on the SII Integrity Line, the whistle-blower automatically receives an acknowledgment of receipt. If it is an anonymous report, they are asked whether or not they wish to remain anonymous for the rest of the processing. In addition, they are invited to provide any information and documents to support their initial report. The whistle-blower is involved in the investigation process only for the verification of the reported facts. The investigation process, its content, and the resulting report are strictly confidential, including towards the whistle-blower.

6.2. Assessment and processing of the report

The SII Ethics Committee, or as the case may be, the Local Ethics Committee, will evaluate each report in confidence to see if it falls within the scope of the Platform. If a report is clearly not related to the Platform, lacks seriousness, is an abusive or slanderous accusation, or contains unverifiable information, it will be considered inadmissible and destroyed without delay. The author shall be informed of this and advised to use the usual internal communication channels (such as going through their hierarchy, employee representatives, or Human Resources).

When a report falls within the scope of the Platform, the SII Ethics Committee or, as the case may be, the Local Ethics Committee will conduct any necessary investigation to verify if the reported facts are true and to preserve the evidence. The Ethics Committee may conduct the investigation itself or delegate it to someone with relevant skills, including an external advisor. All individuals involved in the investigation are legally bound to keep the identity of the whistle-blower, the Concerned Person, any mentioned third parties and the reported facts confidential. Breaking this confidentiality is punishable by law.

It is recalled that, if one of the Authorized Persons is the subject of the Report or is directly or indirectly involved in the reported facts, he/she shall automatically be excluded from the reporting and handling process.

The SII Ethics Committee, or, as the case may be, the Local Ethics Committee and any person they decide to involve or delegate to take care of some or all of the verifications and conduct all investigative actions that are legally permissible, such as:

- copy and/or consultation of any document, file, email or information, regardless of its form and medium, appearing on workstations, professional

email systems, and any other computer or other tool made available to Employees by SII (hard drive, USB key, laptop, drive, paper, etc.), in the absence of their user. However, SII may not access those marked as private or personal except in the presence of the relevant Employee or with their prior consent.

- monitoring of the connection data of Employees.
- use of forensic tools, including keyword searches, scoring and profiling processes as well as personal document, file, email and information sorting processes.
- conducting interviews with relevant Employees.
- conducting an internal investigation.

The Report, including any Personal Data it contains, may be communicated by the SII Ethics Committee or, as the case may be, the Local Ethics Committee to any person capable of contributing to the investigation due to their skills, including any external advisor, for the purpose of verifying and processing it.

Once the verification process is complete, the SII Ethics Committee or, as the case may be, the Local Ethics Committee shall formalize an investigation report. This report shall contain, in addition to the results of the verification process, a description of how it was conducted. This report and its conclusions shall be presented to the executive management, which shall decide on the appropriate action to be taken. Any disciplinary or legal action will be taken in accordance with applicable laws.

The presentation of the report to the executive management marks the end of the verification process and its closure.

The whistle-blower will be informed in writing by the SII Ethics Committee or, as the case may be, the Local Ethics Committee of the action taken on the Report within a reasonable period not exceeding three months from the receipt of the Report or, without an acknowledgement of receipt, three months from the expiry of a period of seven working days following its submission. If the verification process takes longer than three months, the whistle-blower shall be informed before the end of this period.

6.3. Information of the Persons Concerned and Third Parties Mentioned in the Report:

The SII Ethics Committee or, as the case may be, the Local Ethics Committee or an authorized person also informs the Concerned Person targeted in the report, as well as any third parties mentioned, about their rights to access, rectify, and obtain information about their personal data. However, If there is a need to preserve evidence or for the investigation, the Concerned Person and any third parties mentioned will only be informed after such measures have been taken. This is done in accordance with the relevant legal requirements. The Concerned Person and the third parties involved in the Report have the possibility to give their explanations and to be informed of the identity of the persons in charge of verifying the reported facts. They are informed of the conditions for exercising

their rights of access, rectification, deletion and opposition to the processing of their personal data.

7. PROTECTING THE PERSONAL DATA COLLECTED AND PROCESSED UNDER THE SYSTEM

7.1. Data processed on the Platform

Only the categories of Personal Data defined in this Guide may be processed and collected on the Platform.

At all stages of the process, SII ensures that only necessary Personal Data is collected and processed.

7.2. Purposes of processing Personal Data

The Platform aims to collect and process reports made by any Interested Person, including the actions taken in response to them.

Authorized Persons carry out various processes (collecting Personal Data, recording interview minutes, analyzing Personal Data, compiling reports, etc.) with the following objectives:

- collecting the report and verifying whether it falls within the scope of the Platform.
- verifying the validity of the report, if necessary through an internal investigation.
- taking appropriate actions, which may include organizational, disciplinary, judicial, or other measures, based on the results of the report investigation.
- ensuring the defence of the company's interests before the authorities and courts that may be appraised of the facts brought to the attention of the company through the Platform.

Only Personal Data that is necessary for the above purposes is collected and processed.

7.3. Recipients of Personal Data collected and processed on the Platform

Only authorized persons, members of the SII Ethics Committee, or, as the case may be, the local ethics committee and external advisors solicited to assist in the investigation and

processing of the Report, are recipients of the Report and related Personal Data. They are bound by a reinforced obligation of confidentiality.

7.4. Alert Register

The SII Ethics Committee, or, as the case may be, the Local Ethics Committee, maintains an electronic Alert Register, which can only be accessed by its members through a unique identifier and password. Personal data in the register is kept in compliance with existing regulations on data protection.

7.5. Duration of retention of Personal Data

The data collected in relation to a Report which does not fall within the platform's scope of application shall be destroyed without delay or archived after anonymization.

Personal data relating to a Report which falls within the platform's scope of application and to which no further action is taken are archived no later than two months after the end of the verification actions and closure of the Report. Then they are anonymized at the latest 2 years after the end of the verification actions and the closure of the Report.

Where disciplinary proceedings or legal proceedings are initiated following a Report, the related personal data is kept until the end of the proceedings or the limitation of appeals against the decisions taken following the Report. Archiving will be done after anonymization in a restricted access area in the SII administrative premises.

7.6. Security and Privacy

SII takes physical, organizational and technical precautions to preserve data's security, both when it is collected and when it is processed or stored.

Appropriate security and confidentiality measures have been put in place. In particular, the following guarantees are provided:

- The SII Integrity Line platform encrypts the data communicated and exchanged, which is only transmitted through the the SII Integrity Line's secure server.
- Authorized Persons are subject to an enforced obligation of confidentiality.
- Access to the Report is limited to Authorized Persons only.
- No person other than the Authorized Persons can access the SII Integrity Line containing the information collected during the implementation of the Platform.
- Only members of the Ethics Committee have permanent access to the SII Integrity Line.

- As an additional security measure, the IT staff of SII involved in access rights to computer directories and messaging is also subject to an enforced obligation of confidentiality.

7.7. Rights relating to personal data

Personal Data collected through the Platform is processed in accordance with applicable legal and European regulations on Personal Data protection.

Any Person Concerned by the Personal Data collected as part of the System has the right to access, rectify and delete the Personal Data concerning him/her by contacting directly the SII Data Protection Officer (DPO) at the following address: dpd@sii.fr, indicating in the subject of the email "Request for access to Personal Data concerning me".

Exercising this right does not give the person exercising it access to personal data relating to other natural persons.

The right to correction, provided for in Article 16 of the GDPR, and by the privacy legislation applicable in Canada, may, within the framework of the System, be exercised only to rectify factual data, the material accuracy of which can be verified by SII on the basis of evidence, without erasing or replacing any data initially collected, even if it is erroneous. The right to erasure is exercised under the conditions provided for in Article 17 of the GDPR.

Any Person Concerned also has the right to make a complaint to the competent supervisory authority in the event their personal data is misused. In France, the competent authority is the CNIL (Commission Nationale de l'Informatique et des Libertés de France), which can be contacted by any concerned person (3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07).

8. MISCELLANEOUS

8.1. General Policy

SII expects all its Employees to treat any breach of SII's internal rules or the law seriously and diligently. All Employees are required to cooperate fully and assist in the investigation and measures relating to such breaches.

8.2. Effective Date and Amendment of the Guide

This Guide will come into effect as soon as the formalities required by local Labour Code (in France, informing and consulting the Social and Economic Committee (SEC)) have been completed.

Modifying this Guide is subject to the formalities provided for by the local Labour Code and to the information conditions provided for by the French Data Protection Act (in France only).

8.3. Updates

The system described above will be subject to regular evaluations. It may be modified, if necessary. In this case, the Guide will be adjusted and the new version will be brought to the attention of all known Interested Person(s).

9. INFORMATION AND CONTACT PERSONS

Any Interested Person may also contact the SII Ethics Committee directly for any questions relating to the Whistle-blower Alert System and Ethics Policy via digital communication using the "Ask a question" function of the internal alert system (SII Integrity Line).