



SPEAK UP! Misconduct and Non-Compliance Reporting

Privacy Notice



This privacy notice is designed to provide you with clear information about the manner in which Sanofi Winthrop Industrie (SWI), where applicable, other entities of Sanofi Group and third-party vendors operating the **Speak Up! Misconduct and Non-Compliance Reporting Program** will process your personal data for the purpose of receiving, managing, investigating, closing reports and concerns and, where necessary, take corrective measures.

This Program handles various types of reports including but not limited to allegations of potential violations of laws, regulations, employee misconduct or employee breaches of [Sanofi's Code of Conduct](#).

Reports are assessed in accordance with Speak Up, Sanofi Code of Conduct and standards to ensure consistency, coherence, fairness in treatment and adequate resource allocation at group level.

Sanofi Winthrop Industrie acts as data controller for the implementation and management of the Speak Up! Misconduct and Non-Compliance Reporting Program.

Depending on the nature of the allegations and sensitivity of cases, other entities of Sanofi may process your personal data. For example, where there is an investigation concerning an employee, the local employing entity will process personal data related to the case. Depending on the circumstances, Sanofi entities may act as joint controllers.

Individuals whose data is processed by Sanofi may refer to the “*Who to contact for queries*” section below to know more about the data controller for their case.

WHY WE PROCESS PERSONAL DATA

Speak Up! Misconduct and Non-Compliance Reporting Program enables employees, contractors, business partner, supplier, value chain worker, and stakeholder to confidentially raise *allegations of potential violations of laws, regulations, employee misconduct or employee breaches of Sanofi's Code of Conduct or internal procedures*. The program is designed to foster psychological safety and trust while ensuring all reports are handled with strict confidentiality and in full compliance with applicable privacy and data protection requirements.

The **Speak Up! Misconduct and Non-Compliance Reporting** objectives are to:

- Enable any person connected to Sanofi to report, in good faith, allegations that may constitute a violation of applicable laws, Sanofi's Code of Conduct or internal procedures
- Ensure the proper receipt, triage, investigation and closure of reports in a confidential and impartial manner
- Where applicable, protect whistleblowers against any form of retaliation
- Where applicable, fulfil Sanofi's legal obligations as a multinational group operating across multiple jurisdictions

Sanofi processes your personal data based on applicable legal obligations (E.g. EU Directive 2019/1937 on the protection of persons who report breaches of Union law, French Law No. 2022-401, the Sarbanes-Oxley Act (SOX) and the Dodd-Frank Act), in particular to detect misconducts (E.g., corruption, influence) and report any crime or violation of laws.

In case no applicable legal obligation applies, Sanofi relies on its legitimate interest to investigate and address reports to ensure compliance with its Code of Conduct.

WHOSE PERSONAL DATA IS PROCESSED

This notice applies to three categories of individuals whose personal data may be processed in connection with a report:

- **Reporting persons (E.g. Concern Raiser, Reporters, Whistleblower)** - all persons submitting a report or raising a concern, including: any reporter reporting in good faith, current or former employees, external parties using the Speak Up portal (competitors, vendors, members of governing bodies, facilitators), contractors.
- **Impacted Person** – any person who may have been affected / impacted by the alleged wrongdoing.
- **Subjects of reports** - any person whose conduct or actions are the subject of a report.
- **Witnesses and any other** - any person mentioned in the course of a report or investigation or identified by the investigation team as someone who may have / may have had information in connection with the allegations that are being investigated.

WHAT PERSONAL DATA IS PROCESSED

In order to operate the **Speak Up! Misconduct and Non-Compliance Reporting Program**, the following categories of personal data are processed a case-by-case basis:

Personal data relating to Reporting person:

- Identity and contact information: name, job title, entity, professional contact details (when shared by the Reporting person)
- Personal data contained in Report content: description of the facts reported, dates, locations
- Personal data contained in supporting documents or evidence attached to the report
- Secure reference code enabling anonymous case tracking and communication with the investigation team

Personal data relating to Impacted person:

- Identity and contact information: name, job title, entity, professional contact details (when shared by the Reporting person or when made available during the investigation)
- Personal data contained in Report content: description of the facts reported, dates, locations
- Personal data contained in supporting documents or evidence attached to the report

Personal data relating to Subject(s) of the report:

- Identity and professional information: name, job title, entity, location (when shared by the Reporting person or when made available during the investigation)
- Personal data contained in description of the facts alleged, dates and circumstances as reported
- Personal data contained in response or position provided, where applicable, during the investigation

Personal data relating to WITNESSE(s) and any other(s):

- Identity, where mentioned in the report or identified during the investigation
- Personal data contained in information relevant to the assessment or investigation of the report

Technical and case management data insofar as it constitutes personal data:

- Case reference number
- Case status and tracking information
- Appendices and documentation attached to the case
- Communication with the Reporting Person

- Investigation timeline and milestones
- Case closure information

Important – what the Speak Up! Misconduct and Non-Compliance Reporting does NOT collect: the following types of data are not collected for the purposes of investigating reports under Speak Up!:

- IP address
- MAC address
- Access timestamps
- Cookies or trackers on the reporting person's terminal
- Metadata from documents transmitted through the platform

Speak Up! Misconduct and Non-Compliance Reporting Program is confidential by design. It should be noted that the Reporting person can decide to remain fully anonymous when reporting through Speak Up! under the selection “Report Anonymously”.

WHO HAS ACCESS TO YOUR PERSONAL DATA

Internally at Sanofi, access is granted on a strict **need-to-know basis** to specifically identified recipients:

Ethics and Business Integrity (EBI) Investigations:

- EBI Officers - acting as local relays, in particular for reports submitted in person or by post, and for ensuring compliance with local regulatory requirements
- EBI Officers can also conduct investigations into specific alerts that are referred to them by the Lead Investigators or GT&I team
- Global Triage & Investigations (GT&I) team - responsible for receiving, triaging and coordinating all reports submitted through Speak Up
- Lead Investigators (members of EBI global team) - members of the global investigation team who are responsible for defining the investigation strategy, conducting and / or supervising the investigation, documenting the findings, conclusions and outcomes

Human Resources (also known as People & Culture or P&C):

- Head of People Excellence Partners - for managing disciplinary actions following investigation
- People Business Partner (PBP) Local - for supporting corrective or disciplinary action decisions
- P&C MCO (People & Culture Director Multi-Country Organization)- for oversight of disciplinary actions

Cross-functional Teams :

- EBI Officers and Local Compliance Committees - acting as local relays, in particular for reports submitted in person or by post, and for ensuring compliance with local regulatory requirements
- Local Disciplinary Committee - for collective decision-making

Sanofi may also disclose personal data, on a case-by-case basis, and on strict **need-to-know basis** to other identified employees of the Sanofi group entities:

- **Direct Manager of an employee** - for decision-making on corrective or disciplinary actions
- **Employee Outcomes Committee (EOC)** - for US disciplinary cases
- **Legal function** - where attorney-client privilege is applied in anticipation of potential litigation or when the matter requires a legal expertise
- **Subject Matter Experts** – to provide support on specific cases upon the initiative of the Lead Investigator
- **Executive Compliance Committee (ECC), Audit Committee, Board of Directors, Local / Regional Compliance Committees** - receive aggregated statistics, for oversight purposes
- **Head of Procurement Risk Management / Human Rights** - for supplier, partner, and value chain worker concerns

Externally, your personal data will be disclosed to third party service providers acting as data processors under the responsibility of Sanofi Winthrop Industrie:

- **The Speak Up! Helpline external service provider (Navex)** on behalf of and in accordance with the instructions of Sanofi Winthrop Industrie. This provider is bound by strict contractual obligations covering processing purposes, security measures, data return and deletion, and transfer mechanisms
- **Vendors used on a case-by-case basis to support the investigations (e.g. consultants, law firms and associated digital solutions used to support investigations)** on behalf of and in accordance with the instructions of Sanofi. These providers are bound by strict contractual obligations covering processing purposes, security measures, data return and deletion, and transfer mechanisms.

Where disclosure is required by applicable law, personal data is disclosed to **Judicial or regulatory authorities**, with prior notification to the reporting person where legally applicable.

HOW WILL YOUR DATA BE USED?

Reports submitted through the Speak Up! **Misconduct and Non-Compliance Reporting Program** are processed as follows:

- **Triage:** every report is assessed by Global Triage & Investigations (GT&I) team, which determines the appropriate track, or a standard track for all other reports
- **Acknowledgment:** the reporting person receives an acknowledgment of receipt within **7 working days** of submission
- **Investigation:** a Lead Investigator is designated and conducts the investigation in accordance with the principles of confidentiality, impartiality, objectivity and proportionality. The individuals involved are informed as soon as the collection of evidence allows, without compromising the investigation. At the conclusion of an investigation, information may be shared with a small group of key stakeholders including P&C in order to decide on any corrective and disciplinary action or programmatic improvements required
- **Communication:** Reporting person receives regular feedback and is informed when the investigation is completed and case is closed. Depending on the local regulations, specific timelines may be applicable. The persons involved are informed of the outcome within the limits of confidentiality and data protection requirements.
- **Root cause analysis and improvements:** At closure, GT&I and / or Lead Investigator conduct root cause analysis and programmatic improvement assessments, reporting anonymized findings to relevant stakeholders to prevent recurrence and enhance the system.

For identified whistleblowers, upon completion of the investigation, some of the Reporting Person's information may be processed to assess if any retaliation was experienced as a result of reporting concerns of potential misconduct in good faith.

HOW LONG WE RETAIN YOUR PERSONAL DATA?

Personal data is retained in accordance with the following differentiated retention periods:

Personal data contained in Different Types of Report	Retention period
Out of scope (not relevant to the Speak Up! Program)	12 months following closure
Investigations without judicial or disciplinary proceedings	6 years following closure
Investigations with judicial or disciplinary proceedings initiated	Until the end of proceedings and expiry of all applicable appeal periods
Aggregated data	Unlimited retention for statistical purposes

TRANSFERS OUTSIDE OF THE ECONOMIC EUROPEAN AREA

Sanofi is a multinational Group. As such, Sanofi Winthrop Industrie will transfer your personal data to entities of its Group or to third-party partners outside of the Sanofi Group. Such Sanofi or non-Sanofi entities may be located outside the European Economic Area, in countries where personal data legislation does not necessarily offer the same level of protection or in countries not recognized as offering an adequate level of protection.

In particular, the external service provider operating the Speak Up! Program may process data outside the EEA. To ensure an adequate level of protection of your data, those transfers are safeguarded in accordance with the requirements of the country of origin of such transfers, and in the present case:

- Standard Contractual Clauses of the EU Commission
- Binding Corporate Rules

WHAT ARE YOUR RIGHTS CONCERNING YOUR PERSONAL DATA?

Subject to the legislation applicable in the country you are in, you may be entitled to:

- Have access upon simple request to your Personal Data. In that case you may receive a copy of such data unless it is directly available to you
- Obtain a rectification of your Personal Data should your Personal Data be inaccurate, incomplete, or obsolete
- Obtain the deletion of your Personal Data in the situations set forth by applicable data protection law ("right to be forgotten")
- Object to the processing of your Personal Data, where your Personal Data has been collected and processed on the basis of the legitimate interests of Sanofi
- Request a limitation of the data processing in the situations set forth by applicable law
- Request that some of the Personal Data you provided to us is brought to you, or to another data controller, in a commonly used, machine-readable format

Please note that, in accordance with **Article 23 of the GDPR**, the exercise of certain rights — in particular the right of access and the right to erasure — may be restricted during an ongoing investigation in order to protect its integrity, prevent obstruction, and safeguard the rights and freedoms of other persons involved.

Also, and while we suggest that you contact us beforehand, you are entitled to lodge a complaint with [your local Data Protection Authority](#) regarding the processing of your Personal Data.

If you would like to exercise any of these rights, please contact us as described in the "*Who to Contact for Queries*" section below.

WHO TO CONTACT FOR QUERIES?

In order to exercise your rights as set out above, or for any other queries concerning the processing of your personal data including the data controller for your case, please go to [this webpage](#).

Last update: July 2026