Firmenich
for good, naturally

EFFECTIVE DATE: 01/06/2022

OWNER OF THE POLICY: GENERAL COUNSEL

SPEAK UP POLICY

VERSION 4

FOR EXTERNAL AND INTERNAL USE

I. PURPOSE

The purpose of this Policy is to explain how the Firmenich Speak Up network works, including:

a) to whom the Policy applies;
b) the types of concerns that should be reported;
c) the available channels within Firmenich (and outside of Firmenich) for reporting concerns;
d) how the Speak Up reports are handled, and
e) Firmenich's protection against retaliation for anyone who reports a concern in good faith.

Firmenich is committed to conducting business with integrity and fairness, in line with our values and the law. We believe that being able to raise concerns safely and without fear of retaliation is key to sustaining a safe and secure work environment, ensuring our business success and protecting the employees and Firmenich against wrongdoings. The quicker we know, the quicker we can act.

Remember, in certain jurisdictions, local law may impose stricter standards than those set out in this Policy, and vice versa. In all cases, the stricter standards will apply.

II. SCOPE

What is a valid concern that should be reported?

Anyone (e.g., co-workers, suppliers, external staff, former co-workers, future co-workers, consultants, third parties related in any way to Firmenich as suppliers, clients etc.) who sees, hears or experiences a violation of our policies or the law is encouraged to speak up and report their concerns in good faith.

Examples of such situations include:

- a situation contrary to the Firmenich Code of Ethics and its policies under which we operate
- a violation of the law or regulations, whether actual or potential
- a criminal activity
- a situation which could present a threat or cause serious harm to public interest
- a violation relating to human rights or fundamental freedom violation
- discrimination, harassment or bullying
- a violation relating to health and safety or to the environment
- retaliation against anyone for speaking up in good faith

Good faith reporting is where the person reporting the concern has reasonable cause to believe in the truthfulness of the information given, and the report is made without malice or consideration of personal benefit, even if it later appears that they were mistaken. If you realize, after having made a report, that you were mistaken, you must immediately inform the Business Ethics team.

Do not use this Policy:

- To report events presenting an immediate threat to life or property. If you need emergency assistance, please contact your local authorities or call your country's emergency phone number.
- For any grievances you may have in relation to your terms of employment.
- To settle personal or legal disputes.
- To make accusations which you know are false. Doing so may lead to disciplinary measures.

III. POLICY STATEMENTS

No retaliation

Retaliation is a deliberate adverse employment/business action taken against anyone because of reporting a concern or supporting a report. Examples of retaliation can include:

- Firing, demoting or transferring an employee
- Giving an employee undesirable tasks at work
- Reducing an employee's pay or denying the employee a bonus or raise
- A sudden work schedule or location change
- An unwarranted negative employment reference
- Stopping a business relationship with a third party (e.g. a supplier)
- Any other conduct that could have the effect of discouraging a reasonable worker /business partner from making or supporting a complaint

We understand that the decision of speaking up is difficult, and Firmenich will not retaliate, and will not tolerate retaliation, against any individual who reports a valid concern in good faith or who participates in the following up of such a concern. Any act of retaliation may lead to disciplinary measures or legal actions.

If you experience retaliation for reporting or supporting a report of a concern, report it immediately. If you experience retaliation from a manager or the internal resource to whom you originally reported, report the retaliation to a different internal resource.

Confidentiality is key

All allegations will be treated as confidential and privileged to the fullest extent permitted by law. Firmenich will exercise particular care to keep confidential the identity of any reporter. If it proves impossible to investigate the reported allegation without revealing the reporter's identity, this will be discussed with you and the information will be handled sensitively.

All Firmenich employees who are in any way involved in the follow-up of a reported concern are expected to keep all information obtained in confidence to the extent possible and are not to disseminate such information further without obtaining authorization from the Head of Business Ethics or a person appointed by him/her.

Personal Data

As set out in Firmenich's Employee Information Notice and our Corporate Employee Personal Data Policy, Firmenich may process personal data to follow-up and, if needed, investigate a concern reported via the Speak Up framework, in compliance with local laws and regulations. In-scope personal data may include personal details (such as name, email address, telephone number), employment details (such as job description, job location, line management details, contract length) and any other personal data provided

within a report. We may also process the personal data of any individual referenced within a report. For more information on the way we process any personal data provided through the Speak Up Framework and your rights, please visit the Data Protection and Privacy Notice.

a) Staff permitted to have access to the personal information must be strictly limited on a need to know-basis. Staff with access must be subject to a reinforced obligation of secrecy and access to the whistleblowing reports must be monitored whether in electronic or paper form.
b) From a technical point of view, the requirements of access control need to be fully implemented by: effectively limiting and controlling who has access to whistleblowing cases, accessing logs and regularly reviewing both access to the logs and the access rights.
c) Encryption needs to be specially considered due to the high needs of confidentiality of this information. Notwithstanding the use of encryption, safeguard mechanisms need to be implemented to allow access to the information when needed (shared keys, recording and safe keeping of passwords...).

For detailed information on how Firmenich collects, uses and discloses personal data in connection with the Speak Up Policy, please refer to **Appendix 1.**

IV. POLICY REQUIREMENTS

How to speak up?

As part of its Speak Up framework, Firmenich offers different mechanisms for reporting wrongdoings. The reporter can decide which mechanism they feel more comfortable to use, but in all cases the same principles of confidentiality, investigation and non-retaliation are followed.

These reporting mechanisms are:

A) **Reporting to the Head of Business Ethics:** The Head of Business Ethics can be contacted by e-mail or other Firmenich communication tools.

B) **E-mail** to ethics@firmenich.com: Only the Business Ethics team has access to this mail box and will assign an investigator not involved in the reported case to conduct the investigation.

C) **Local or HR Management:** The manager can be contacted by e-mail, in person or by any other Firmenich communication tools.

D) **Speak Up platform (Hotline):** It can be reached by phone or web-form and it is available 24 hours a day, 7 days a week. You can reach the platform, including the phone numbers here. This platform is hosted by an external company and only a few designated people in Firmenich have access to the reports, and only to those parts relevant to them.

Please note, in some countries there are, due to legal reasons, specific requirements in how the Speak Up channel can be used (e.g. in line with the EU Whistle-Blower Directive, local designated persons are available in specific affiliates for local report intake). The platform is updated accordingly regularly.

How to do it

No matter which channel you choose to use to raise your concern, you should provide as much information as possible in order to facilitate the investigation of such a concern. These include:

- A detailed description of the situation of concern as well as antecedents and/or examples
- Names of people potentially involved, dates, places

- Any supporting facts and documents related to the concern
- When and how you became aware of the matter
- Your contact details

Should you decide to use the Speak Up platform (Hotline), you will receive a user ID and password to follow up on the progress of your reported concern. To facilitate the follow-up, you are strongly encouraged to follow up and to respond to any questions that may be raised through the Speak Up platform (Hotline) promptly.

Can I report anonymously?

Subject to any local legal restrictions that may apply, you may raise your concerns anonymously.

Please bear in mind that it is more difficult to examine anonymous reports and enough detail must be provided to proceed with, and properly conduct an investigation. If you are concerned about possible retaliation please see above.

What happens next:

1. The receiver will acknowledge receipt of the concern raised within 7 working days. This time may be extended if the response requires translation.
2. No matter which method you choose to use, the person handling the case will decide on next steps, which could be:

- Opening an investigation
- Asking for further information
- Not taking further action for lack of information / facts to proceed
- Handing over the report to relevant law enforcement authorities

The person handling reports is expected to:

- Be impartial
- Be bound by a strict confidentiality obligation. The elements allowing the identification of the reporter cannot be divulged, except to the legal authorities, without their consent
- Conduct the investigation as per the Investigation Guidelines
- Provide periodically updates on the investigation to the reporter, until the closure of the case
- Provide feedback within 90 days of filing the report

The investigation will be registered diligently and securely by the investigator and the records will be kept confidential, as per the guidelines of Personal Data Protection.

External reporting mechanisms

Firmenich encourages all individuals to report any concern of misconduct internally first, but if there is no speedy or appropriate resolution of the concern, you have the option of going to the relevant authorities.

Transparency and Communication

The General Counsel and/or the Head of Business Ethics (or a person appointed by either of them) will provide periodically a program overview to Global and Local Ethics Committees. Such overviews will include statistics, brief summaries of allegations, investigation outcomes and corrective measures. We may

also publish similar information in external reports. All such reports shall be made in compliance with confidentiality requirements and applicable laws.

V. EXCEPTIONS

Exceptions to this Policy must be approved by the Policy owner.

VI. POLICY MANAGEMENT

Policy Change Log:

Version	Date of issue	Effective date	Purpose of change
1	**31.07.2017**	**31.07.2017**	• Creation of the Hotline
2	**01.05.2018**	**01.05.2018**	• Update regarding Personal Data
3	**15.02.2020**	**01.03.2020**	• Clarification of the Scope, Investigation and Reporting sections • Listing also the other reporting channel and the priority in their use • Extending the protection from retaliation and confidentiality requirements
4	**01.06.2022**	**01.06.2022**	• Update re Scope, Policy Statements (clarification of intake methods, explanation of the process, external mechanisms, data privacy)

Questions and feedback regarding this policy should be submitted to the Business Ethics function via ethics@firmenich.com.

VII. SUPPORTING DOCUMENTS

Code of Ethics
Diversity & Belonging Policy

VIII. APPENDIX

Appendix 1 Speak Up Policy Privacy Notice

This Privacy Notice explains how Firmenich collects, uses and discloses personal data in connection with the Speak Up Policy. Personal data means any information in any format relating to an identified or identifiable individual (for more information on this definition please visit our Corporate Employee Personal Data Policy).

Please read this notice carefully as it describes in detail the rights and responsibilities regarding processing of your personal data (supplementing our Corporate Employee Personal Data Policy and the Employee Information Notice).

Personal Data We May Process When You File a Report

You remain in control of what personal data (yours, or of another individual) is provided under a report. No personal data will be processed providing you enter no personal data in the report and you do not enter your email address to receive email updates.

This way, Firmenich will solely collect and process personal data you specifically provide under a report, and to the extent necessary to pursue our legitimate interests in preparing a report, conducting an investigation and responding to the concern when you speak up using any of the different mechanisms provided under the Speak Up framework. The personal data processed within the investigation will be limited to the data strictly and objectively necessary to verify the allegations made.

In connection with a report, depending on the information you provide, we may collect and process personal data, including the identity, job title, location (affiliate) and (corporate) contact information of:

- ✓ the individual submitting the report;
- ✓ the individual who is the subject of the report;
- ✓ other individuals with information relating to the report (“witnesses”); and
- ✓ the individuals responsible for investigating the report.

In addition, personal data may be included in:

- ✓ the facts that are reported;
- ✓ evidence gathered in the course of the investigation, including reports generated as part of the investigation; and
- ✓ any response taken by Firmenich as a result of the report.

It is not intended that Firmenich collects or processes sensitive personal data (i.e., information about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning sex life or sexual orientation) or criminal convictions and offences. To the extent such data is intrinsic to the facts that have been reported, we will seek to minimize any resulting collection and further processing of such data and ensure appropriate safeguards are in place in accordance with applicable regulation.

Who has access to the report?

Depending on the nature of the alleged facts in the report, these may be forwarded for review to relevant Firmenich stakeholders such as representatives from the Legal and Compliance Department, Human

Resources, IS or other relevant departments. We may also use external advisors in reviewing a reported concern or allegation of misconduct (under appropriate confidentiality obligations).

Firmenich may disclose the reporter's identity as may be required by law, such as in response to a court or administrative order or equivalent legal requirement or to relevant persons involved in conducting an investigation or any subsequent adjudication.

Data Transfers

We are part of a global organization. To the extent permitted by applicable law, your personal data may be transferred to, stored or accessed by FIRMENICH staff located in your affiliate or elsewhere for the purpose of managing the report and investigating an allegation. Only restricted and authorized staff will have access to the report.

In addition, our third-party Speak Up platform (Hotline) service provider is located in United States (please visit their Privacy Notice). Firmenich and our third-party Hotline service provider are subject to and comply with the provisions of GDPR and any applicable data protection regulation. When your personal data is transferred to (or accessed from) a country outside the EU for which the European Commission has not issued an adequacy decision, we will ensure that appropriate safeguards are implemented to protect your personal data in accordance with applicable law. This may include (intra-group) data transfer agreements incorporating the European Commission's Standard Contractual Clauses, pursuant to article 46 of the GDPR.

Security and Retention

We have implemented technical and organizational measures to protect your personal data. We will endeavor to destroy or anonymize (i.e., all personal identifiers will be removed) personal data contained in a report within a reasonable amount of time after the conclusion of the relevant investigation, unless the investigation leads to disciplinary or legal proceedings, in which case we may need to retain your personal data until the conclusion of those proceedings and the period established under applicable law.

Your Rights

Subject to applicable law, you may have the right to request access to and receive details about the personal data we maintain about you in connection with a report made via the Speak Up framework using any of the different mechanisms for reporting wrongdoings. You also may have the right to request that certain personal data about you be rectified, erased or restricted, in accordance with applicable law. You also may have the right to object at any time, on legitimate grounds, to the processing of your personal data in the context of a report. We will respond to your questions or complaints relating to the processing of your personal data. If you are not satisfied with our responses, you may consult the data protection authority of your country.

The exercise of your rights may be restricted as necessary to protect others in the context of a particular allegation.

Contact Us

If you have any questions or comments about your personal data rights under the Speak Up Policy, or if you would like to exercise your rights of access, correction, erasure, restriction or objection to the processing of your personal data, please contact data.privacy@firmenich.com.