



SpeakUp Privacy Notice

1. Introduction & Purpose

At dsm-firmenich we are committed to being always transparent in our handling and processing of any personal data in accordance with applicable privacy and data protection regulations.

This Privacy Notice explains how we handle the processing of personal data that we collect from you, or that you provide to us, in the context of SpeakUp reports issued via the dsm-firmenich SpeakUp platform (indistinctively, “the **SpeakUp Platform**” or “**Platform**”).

'SpeakUp®' Platform is a Software as a Service (SaaS) solution provided for dsm-firmenich by People Intouch B.V. (a company incorporated under the laws of Netherlands), that makes it possible to report about unlawful or unethical behavior. The Platform is provided to enable all dsm-firmenich employees and third parties to raise concerns about possible misconduct or risks as described in the Speak Up website.

dsm-firmenich is the data controller of any personal data you provide to us and People Intouch B.V. serves as a data processor (in its condition of software provider).

The security of anyone using our platform privacy is important to us. We want you to feel safe while using our SpeakUp Platform and ask you to read and acknowledge the following information concerning the collection of personal data.

2. Legal basis

The processing of your personal data is carried out on the basis of Art 6 (1) c GDPR to **comply with the 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 and the relevant national implementing laws.

In addition, the processing of personal data of persons, affected and involved in the reporting process is based on the **legitimate interest** of dsm-firmenich-as data controller- to prevent, detect, investigate and remedy any reported wrongdoing (Art 6 (1) f GDPR).

3. What personal data and information is collected and processed?

In order to file a report, we will ask you to provide as much relevant information as possible, which should be detailed, objective and directly related to the subject matter of the report.



The report will include this information (as any concern can be raised through the 'Speak Up' process this list is not exhaustive):

- Your contact details, *if you are not reporting anonymously*.
- A detailed description of the situation of concern as well as antecedents and/or examples.
- Names and positions of people potentially involved (including witnesses), dates, places.
- When and how (directly or indirectly) you became aware of the matter.
- Whether steps have already been taken to remedy the situation.
- Whether you have already shared your concern with others.
- Any supporting facts and documents related to the concern.

Please bear in mind that the SpeakUp Platform offers anyone wishing to file a report to dsm-firmenich a free form system, by this meaning that it is up to you to decide which-if any-personal details you want to include in your report or questions. The Platform can be used **anonymously**, in this case your identity or personal details that can identify you are not disclosed to us.

Special categories of personal data may be processed under the exception stipulated in Art 9 (2) g GDPR-although it is not the intention of dsm-firmenich to collect any such data-, unless it is relevant for the report and investigation. Pursuant to Art. 17 of the Whistleblowing Directive, any **irrelevant or excess personal data will be deleted**.

4. Your data protection rights

dsm-firmenich is committed to being transparent about how it collects and uses your personal data and to meeting its data protection obligations, therefore, we comply with the data protection principles when processing (if any) your personal information or any personal information you share with us about any third party mentioned in the report ("data subjects").

Under data protection legislation, data subjects have a number of rights that are applicable under certain conditions and in certain circumstances:

- Access and obtain a copy of their respective personal data.
- Require to rectify (change), without undue delay, incorrect or incomplete personal data.
- Require to delete their respective personal data.
- Request to restrict the processing of their respective personal data if: (a) they contest the accuracy of the personal data being processed, (b) the processing is unlawful and they oppose the erasure of their personal data and request the restriction of their use instead, (c) dsm-firmenich, as being the data controller, no longer needs their personal data for the purposes of the processing, but they have required us for the establishment, exercise or defence of legal claims, and (d) they object to processing pending the verification whether the legitimate grounds of the data controller overrides theirs.
- Request their respective personal data in a portable format.



- Object to the processing of their respective personal data for which we use legitimate interest as a legal basis, in which case dsm-firmenich will cease the processing unless we have compelling legitimate grounds for such processing.

Furthermore, data subjects have the right to lodge a complaint with the (public) supervisory authority, in particular in the Member State of their habitual residence, place of work or place of the alleged infringement.

5. Use of data provided via the SpeakUp Platform- Who can access the personal data?

Concerns shared through the platform are received by the Business Ethics team and shared with appropriate internal partners. When you file a report through the Speak Up website (or call center), you will receive a unique username and select a password. You can then return to the Platform either online or by phone (we encourage you to download the app) to access your original report and add more details or updates.

The receiver will acknowledge receipt of your concern and will manage directly your case or revert to another person/team who will be able to handle it in better condition. Receipt of the report must be confirmed to the reporter within seven days while he or she must be informed of any action taken within three months, as well as the status of the internal investigation and its outcome. You will receive a tracking number to check status and answer follow-up questions.

The person handling the case will decide on next steps, which could be opening an investigation, asking for more information, or not taking further action for lack of information / facts to proceed or because the report does not represent a real or potential breach of policies, laws and/or regulations.

You will receive periodically updates on the investigation, until the closure of the case. In all cases, the investigation will be registered, and the records will be kept confidential.

dsm-firmenich will treat all disclosures of suspected wrongdoing in a confidential and sensitive manner and maintain your privacy. Confidential means that your identity will be shared only with those who have a need to know in order to effectively conduct any investigation and follow-up action (including, if necessary, disciplinary action) on your concern, or where there is a legal requirement to share your identity.

To ensure the privacy of everyone involved, you should only disclose information that is relevant to the concern and avoid providing information not relevant to the concern.

6. Security, disclosure of personal data and international transfer of personal data

dsm-firmenich is committed to protecting your privacy and comply with privacy laws and regulations. dsm-firmenich operates internationally and has locations in various countries within



and outside Switzerland and the European Union. The stored data may only be processed by specially authorised persons within dsm-firmenich as described in this notice.

People Intouch providing the SpeakUp Platform on behalf of dsm-firmenich has taken extensive measures to prevent the loss, misuse and alteration of your personal data. All data on the SpeakUp Platform is encrypted and stored within the EU (Germany and France)). All communication via the Platform is encrypted.

Exceptionally, the data may be accessed from overseas by the abovementioned stakeholders (relevant staff involved) or be transferred by them outside of the EU/EEA or Switzerland (i) where necessary for the investigation (ii) where it is legally required to disclose it to local authorities and courts or (iii) where it is absolutely necessary to protect vital interests of people.

Insofar as this is necessary to fulfil the investigation, specially authorised persons of dsm-firmenich companies located in various regions may also be entitled to inspect the reports (i.e., when the investigation is carried out in the country concerned). Any and all persons authorised to inspect the reports are expressly bound to confidentiality obligations.

Within dsm-firmenich, we have (i) an Intra Group Data Transfer Agreement that protects personal data transferred internationally within the group and is based on the Standard Contractual Clauses of the European Commission and (ii) Binding Corporate Rules.

7. For how long do we store the data?

Dsm-firmenich will keep your personal data for as long as is needed to fulfil our purposes of investigating compliance concerns and documenting our compliance with applicable laws, unless dsm-firmenich is required under applicable regulations to keep your personal data for a longer period.

Different retention periods apply, following our corporate retention policy, if legal proceedings or disciplinary measures are initiated.

The personal data you provide will be kept as long as necessary to process your report, or, if applicable, as long as necessary to initiate sanctions or to meet our legal or financial needs. If judicial or disciplinary proceedings are initiated, the personal data provided will be kept until those proceedings are definitively closed, the issue resolved and during the period permitted under applicable laws.

People InTouch use certain technical information (e.g. IP address) to prevent and detect security threats or other malicious activity. This data will never be used for any other purpose and will be deleted after 3 months, unless this period is extended due to an established act of malicious activity. Neither People InTouch nor dsm-firmenich use cookies or tracking tools.



Personal data relating to a report judged being “inadmissible” or “admissible but not valid” will be removed immediately. “Removed” means that the personal data are completely deleted or adapted in such a way that identification of the person involved is no longer possible (anonymized). dsm-firmenich will take the necessary technical and organizational measures to adequately safeguard personal data against loss or unauthorized access.

Personal data relating to reports that are “admissible and valid” will be kept for two (2) years, unless disciplinary action is taken or court proceedings are filed against a person. In these events, the data will be removed within two (2) years after the disciplinary action or the court proceedings have been finalized.

8. Questions

This Privacy Notice reflects how personal data is processed in the SpeakUp Platform.

Questions regarding this Privacy Notice or our website should be directed to the following email address: ethics@dsm-firmenich.com.

Furthermore, if you have any doubts or concerns regarding how your personal data is handled, please contact our data protection team at privacy@dsm-firmenich.com.