DSM
BRIGHT SCIENCE. BRIGHTER LIVING.

DSM Alert

DSM ALERT

ROYAL DSM WHISTLEBLOWER POLICY

Adopted by the Managing Board of Koninklijke DSM N.V. on June 14, 2004
amended on March 17, 2014
amended on December 18, 2017

This document explains our whistleblower policy and procedure to support our employees and third parties in expressing their concerns about suspected serious misbehavior at or related to activities of DSM (hereinafter the "Policy").

Content

1. General

Today's society expects that persons, who have serious concerns about what is happening at their work, should feel free to report such concerns. In order to protect those persons when reporting their concerns, guidelines and legislation (e.g. in the Netherlands the Dutch Corporate Governance Code and specific legislation for Whistleblowers), have been established.

Within DSM, we wish to maintain the highest standards of business conduct and ethical behavior. We have embedded the opportunity to file a complaint in our Code of Business Conduct and in the DSM Corporate Requirements (together: the DSM Regulations).

We encourage our employees to report any Breach (as defined hereunder) without being worried of any retaliation, punishment or unfair treatment.

This Policy describes what a person should do when he suspects or observes a Breach. Before reporting a Breach, a person always has a possibility to consult an advisor. Also third parties can raise issues under this procedure, using the provided links on our corporate website www.dsm.com.

DSM's Managing Board appointed an officer responsible for handling reported Breaches (hereinafter the "Alert Officer"). The Alert Officer (Senior Vice President Corporate Operational Audit) is supported by the DSM Alert Committee (hereinafter the "DAC"). The DAC consists of the Alert Officer, the VP Corporate Affairs, the SVP Group Legal Affairs and the EVP Group People & Organization. The Alert Officer chairs the DAC. Other designated DSM employees can support the DAC.

2. Breaches

A "Breach" is a violation or the suspicion of a violation on reasonable grounds of any legislation and/or DSM Regulations by any DSM employee, contractor, agent or distributor operating on behalf of DSM or commissioned by DSM. Breaches are not limited to fraud, theft, corruption, discrimination or harassment, but can regard any other ethical or behavioral complaint as well.

For us it is important to know what is happening within our organization. Therefore, we encourage persons to engage in a discussion with colleagues who show behavior considered a Breach. Everyone is also encouraged to report any Breach to his/her management or the Alert Officer.

3. The essentials of whistle blowing

Non-retaliation
We protect any person, who reports a situation or occurrence, which he/she reasonably believes is a Breach. We shall, in no way, harass him/her because of a report. Retaliation against a person for reporting in accordance with this Policy is a serious violation of the Policy itself. If this occurs, the violator will be subject to appropriate disciplinary sanctions. Any such retaliation must be reported to the Alert Officer at once.

Confidentiality
We recognize that individuals who observe a Breach, and wish to report it, will do so under assurance of confidentiality. We will handle all reports confidentially and we equally expect persons reporting a Breach to keep this confidential too.

We do however acknowledge that in some situations the investigation process may reach a point where the person who reported the Breach needs to make a statement or provide further evidence. Under such circumstances, when maintaining someone's privacy hinders finding the truth, we may not be able to guarantee full confidentiality to the reporting person.

We want to avoid anonymous reports, as it can make investigating allegations very difficult. However, if a person feels there is no other way than filing an anonymous report and applicable local law allows for it, we will always take appropriate protective action.

Abuse of the policy
We encourage persons to report Breaches and assume this is done in good faith. If after an investigation Breaches can't be confirmed or can't be substantiated, no action is taken against persons raising such Breaches. We will, however, take appropriate action if the person reporting knows, or could have known that a reported alleged Breach is false. Malicious reports without any factual foundation, will lead to disciplinary action.

4. Reporting levels

4.1 General

There are three reporting levels:

Level 1: Line management
Level 2: Alert Officer
Level 3: Chairman of the Managing Board / Chairman of the Supervisory Board

At each level, all reported Breaches are handled carefully, confidentially and promptly. If a Breach isn't reported at the appropriate level, the person receiving the report will forward it to the appropriate level and inform the reporting person.

4.2 Level 1: Line management

As a general rule, persons should report Breaches first within their own working environment or organization. Open discussion with line management or the local HR business partner is the starting point. If reporting to line management is not possible, because it would be inappropriate or unfeasible, the report can be made at Level 2.

If a specific local complaint procedure is in place, a Breach can also be reported through this procedure and to the persons mentioned in that specific procedure.

The decision by line management is not open for appeal at the next level, being the Alert Officer. In case the handling of the complaint by line management, or the decision taken is in itself considered a Breach, the person can report such case as a new case to the Alert Officer.

4.3 Level 2: Alert Officer

Notwithstanding the procedures mentioned in the previous section, a person should report Breaches directly to the Alert Officer if:

- the Breach relates to any of the following subjects that may harm DSM (not limitative):
  - criminal acts in relation to DSM or our assets, such as fraud or theft;
  - a (potential) danger to the health, safety and security of persons or to the environment;
  - corrupt and dishonest behavior;
  - harassment;
  - discrimination;
  - inappropriate accounting practices, or lack of internal accounting controls;
  - abuse of authority by management; and
  - any other behavior that could have a detrimental effect on our reputation and/or financial position.
- reporting to line management is not possible (because it would be inappropriate or unfeasible).

The role and tasks of the Alert Officer and the DAC are described below in the paragraph "Procedures". If an alleged Breach comes to the attention of the DAC, other than through a report by a person, the DAC has the authority to treat the matter in accordance with this Policy.

A decision taken by the DAC is not open for appeal at the next level, being the Chairman of the Managing Board or the Chairman of the Supervisory Board. In case the handling of a complaint by the DAC, or the decision taken is in itself considered a Breach, the person can report such case as a new case to the Chairman of the Managing Board or to the Chairman of the Supervisory Board.

4.4 Level 3: Chairman of the Managing Board / Chairman of the Supervisory Board

If a Breach is reported concerning the Alert Officer and/or one or more other members of the DAC or a member of the Managing Board, not being the Chairman, the reporting person should report directly to the Chairman of the Managing Board.

If a Breach is reported concerning the Chairman of the Managing Board, then the reporting person should report directly to the Chairman of the Supervisory Board.

5. How to report

Level 2 Breaches are reported to the Alert Officer via the Alert website, by telephone or by e-mail. Level 3 Breaches are directly reported to the Chairman of the Managing Board or the Chairman of the Supervisory Board in writing, depending upon the nature of the Breach.

The person reporting a Breach provides the background, history and reasons for his/her concern, together with names, dates, places and as much other relevant information as possible. We will always try to support persons reporting a Breach to report in their native language, if preferred.

It is not necessary that a person reporting a Breach immediately proves all facts leading to a Breach, but he/she should be able to provide sufficient evidence to substantiate the assumption of a Breach. Individuals are encouraged to report Breaches at the earliest possible stage, in order to take timely action.

6. Procedures

The periods mentioned in this paragraph start on the day following the date on which the report is received at the appropriate reporting level, unless otherwise indicated.

6.1 A report at Level 2

A level 2 report of a Breach is handled by the Alert Officer. Designated DSM persons, within the region where the Breach occurred, may support the Alert Officer. The Alert Officer will take the following actions:

- Confirm the receipt of the report to the reporting person.
- If relevant, arrange an interview with the reporting person to get more details of the complaint.
- Inform the DAC as soon as possible after receipt of a report of a Breach. If the reporting person requests so, his/her name is kept confidential.

The role of the DAC

The DAC decides within ten (10) business days after receipt of a report, whether that report is admissible. A report by the reporting person is inadmissible if:

- The report clearly does not relate to a Breach; or
- The report is not sufficiently substantiated.

If the report is admissible, the DAC investigates the case. The internal investigation may be done by the Alert Officer, a representative of the DAC or another person appointed by the DAC, at its discretion. The person(s) performing the investigation may need to speak to the reporting person to clarify the information provided or may seek additional information from other persons.

When the investigation is finished, the DAC decides whether a Breach has occurred or not. In case of a Breach, the DAC will take a decision and/or provide a solution, or, at its discretion, ask line management to take a decision and/or to provide a solution. The DAC informs the reporting person in writing about the decision of the DAC within ten (10) business days after taking its decision.

If the investigation by the DAC takes more than two (2) months, the Alert Officer informs the reporting person and indicates how long it may take to provide a final response.

Any person involved in an investigation should cooperate with the assigned DAC investigator(s). Withholding relevant information will be regarded as serious misbehavior.

6.2 A report at Level 3

If the Chairman of the Managing Board receives a report, he shall review and discuss this report with another member of the Managing Board who is not subject of that report. The Chairman of the Managing Board will decide within ten (10) business days whether the report is admissible. The criteria for inadmissibility of a report at Level 2 apply equally to reports at Level 3. The Chairman of the Managing Board may involve the Alert Officer, the DAC and other DSM persons, as well as external advisors or institutions in the investigation as required and as far as they are not subject of the report themselves.

The decision whether a Breach has occurred or not is taken within two (2) months after the Chairman of the Managing Board has received the report or – if two months is not reasonable – within an appropriate period. In case of a Breach, the Chairman of the Managing Board will ask the DAC to take a decision or the Chairman of the Managing Board will take a decision himself, together with another member of the Managing Board. The Chairman of the Managing Board informs the reporting person in writing about his decision within ten (10) business days after taking his decision.

If the Chairman of the Supervisory Board receives a report, he shall review and discuss it with the Audit Committee of the Supervisory Board. The Chairman of the Supervisory Board will decide within ten (10) business days whether the report is admissible. The criteria for inadmissibility of a report at Level 2 apply equally to reports at Level 3. The Chairman of the Supervisory Board may involve other members of the Supervisory Board who are not involved in the Breach, the Alert Officer, the DAC and other DSM persons, as well as external advisors or institutions in the investigation as required and as far as they are not subject of the report themselves.

The decision whether a Breach has occurred or not is taken within two (2) months after the Chairman of the Supervisory Board has received the report or – if two months is not reasonable – within an appropriate period. In case of a breach, the Chairman of the Supervisory Board will take a decision and/or provide for a solution himself, together with another member of the Supervisory Board. The Chairman of the Supervisory Board informs the reporting person in writing about his decision within ten (10) business days after taking his decision.

7. Subject of a Report

The Alert Officer may inform the person about whom a report is filed of such a report. In cases where there is a substantial risk that such notification would jeopardize the ability to effectively investigate the reported facts or to gather the necessary evidence, notification to the person about whom a report is filed can be delayed as long as such risks exist.

The information given to the subject of the report will contain the facts of the Breach as reported. He/she will be given the opportunity to provide an explanation, without the name of the person who reported the Breach being disclosed to him/her. The subject of the report may request access to his/her personal data held by the company via the Alert Officer. He/she has the right to have incorrect, incomplete and outdated data corrected or removed.

As soon as the investigation has been concluded, the subject of the report will be informed of any action to be taken as a result of the report. If the person about whom a report was filed is informed that no action will be taken, any suspension or temporary measure that has been imposed on him/her will automatically terminate.

8. Reporting by the Alert Officer

The Alert Officer will provide, at least bi-annually, an overview of the Alert cases to the Managing Board. Likewise, the Alert Officer will also provide an overview of the Alert cases to the Audit Committee of the Supervisory Board, but on an annual basis.

9. Confidentiality

The reporting person, the Alert Officer and the DAC shall keep the final report confidential. Information relating to this report shall only be given to other persons within our company if they need this to execute their tasks under this Policy and/or to implement the conclusions of the investigation. The name of the reporting person will not be disclosed, unless this is necessary for the investigation and/or judicial procedures and only after informing the reporting person.

10. Privacy issues and retention periods

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. The Alert Officer 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.

11. Final provisions

This Alert Policy replaces all previous versions and will be effective as of December 18, 2017. This English version of the Alert Policy will prevail over any other version.

12. More information and contacts

General information: www.dsm.com
Level 2 alerts:

- mail to: dsm.alert@dsm.com
- ☎ +31 45 578 2222 (available 24/7)