

STIBO

Whistleblower Policy

Version: 1.1, June 2024

Author: Legal and ESG/Sustainability

Confidentiality Level: Public

1 Whistleblower Policy

1.1 Summary

A **whistleblower** in any entity under Stibo DX or Stibo Systems (collectively referred to as Stibo Software Group) is a person who raises a concern about illegal or criminal activities or clear and serious violations of internal guidelines or policies of Stibo Software Group, to the extent such violations indicate serious misconduct which may affect Stibo Software Group or which may have a decisive impact on the life and health of individuals. If you become aware of any illegal or criminal activities or clear and serious violations of internal guidelines or policies of Stibo Software Group, you are encouraged to submit a report via Stibo Whistleblower Scheme, which can be accessed through the link below:

***Note** – If nothing happens, please right-click, copy link and paste it in your browser.

<https://stibo.whistleblownetwork.net/>

The Stibo Whistleblower Scheme is at present administered by an impartial third party named Got Ethics A/S.

This whistleblower policy does not suspend or act as a substitute measure for the usual communication between employees and Stibo Software Group's management and/or between Stibo Software Group and its external stakeholders.

Accordingly, in case you encounter issues or problems during your work with Stibo Software Group you are generally encouraged to talk to your manager or your point of contact at either Stibo DX or Stibo Systems. Below you will find information on the whistleblower policy and how it is implemented in Stibo Software Group.

1.2 Purpose of the Stibo Whistleblower Scheme

The purpose of the Stibo Whistleblower Scheme and the associated processing of personal data are the following:

- to prevent and investigate any suspected illegal or criminal actions and any clear and serious violations of internal guidelines or policies of Stibo Software Group as further described above under section 1;
- to highlight the importance of a consistent high level of credibility towards Stibo Software Group's existing and potential employees, customers, vendors, and other stakeholders; and
- to provide a formal and secure procedure for protecting employees that choose to come forward under the whistleblower policy.

This whistleblower policy is annually reviewed to ensure that Stibo Software Group is aligned with current good practices.

1.3 Who may submit information by way of the Stibo Whistleblower Scheme?

You may submit information by way of Stibo Whistleblower Scheme if you are either an existing or former employee, a customer, a vendor or a stakeholder of any entity under Stibo Software Group.

1.4 Anonymity

In order to provide Stibo Software Group with the best possibilities to process any information submitted under the Stibo Whistleblower Scheme, Stibo Software Group recommends that you disclose your identity to us when submitting information via the Stibo Whistleblower Scheme. Stibo Software Group will of course keep your identity in full confidence and not disclose your identity

whether internally or externally, unless required under mandatory law. However, eventually it is up to you whether you decide to disclose your identity or remain anonymous when submitting information via the Stibo Whistleblower Scheme, and any information received by virtue of the Stibo Whistleblower Scheme will be processed whether anonymous or not.

1.5 No adverse employment consequences in relation to reports in good faith

As a whistleblower, you are protected by law against sanctions of any kind due to reporting to the Stibo Whistleblower Scheme in good faith. Stibo Software Group guarantees that the submission of information through the scheme in good faith will not have any adverse employment consequences for or otherwise be used to the detriment of the informant in question. All information, including the identity of the whistleblower, will be treated confidentially as described under section 9.

1.6 Which offences may be reported under the Whistleblower Scheme?

Only information that indicates that one or more employees, management or board members of Stibo Software Group - either actively or by omissions and by virtue of their position(s) in or assignments for Stibo Software Group - carry out illegal or criminal activities or commit clear and serious violations of internal guidelines or policies of Stibo Software Group. This will be done when such violations indicate serious misconduct which may affect Stibo Software Group as a whole or which may have a decisive impact on the life and health of individuals.

For example, this may include economic crime and fraudulent behaviour, including fraud, corruption, forgery, bribery, money laundering, irregularities in respect of financial accounting and auditing and anticompetition. Other examples of incidents that may be reported include cases of environmental pollution, serious violations of occupational safety rules and serious offences against an employee, for instance violence or sexual offences.

On the contrary, less serious misconduct will be disregarded, should it be submitted under the whistleblower policy. Thus, as a general principle information which relates to the day-to-day matters in Stibo Software Stibo Software Group – Whistleblower Policy Page 4 of 6Group's departments such as difficulties in cooperation, incompetence, absenteeism, use of e-mail/internet etc. will not be processed under the Stibo Whistleblower Scheme. The same applies to violations of internal guidelines or policies of Stibo Software Group, to the extent such violations cannot be regarded as serious violations or misconduct as further described above.

1.7 Who will receive the information?

Information submitted to the Stibo Whistleblower Scheme will be made available to the Chairman of the board of directors at Stibo Software Group (hereafter called "the Chairman").

1.8 How will information be used?

The Chairman will review the information and decide whether a formal investigation of the matter at hand should be carried out with a view to consider the appropriate measures.

Upon having carried out a formal investigation, if required, the measures that can be applied by the Chairman are following: (i) dismissal of the information as being unfounded or outside the scope of the Stibo Whistleblower Scheme; (ii) initiation of employment sanctions against the employee(s), manager(s) or board member(s) who are the subject(s) of the report; (iii) filing of a report to the relevant authorities (including the police) of the matter at hand; (v) initiation of a more thorough investigation of the matter at hand and (vi) suggestions as to changes to internal policies or procedures of Stibo Software Group on the basis of the matter at hand.

Collection and processing of personal data submitted via the Stibo Whistleblower Scheme will be conducted in compliance with applicable data protection laws, including but not limited to the Danish

Act on Processing of Personal Data and the EU General Data Protection Regulation, as well as any other relevant applicable legislation. This means that the individual reporting as well as the reported individual has a number of specific rights.

Among others, you may request information about the following:

- If a report regarding you or your actions has been submitted.
- Which individuals have or can have access to the data submitted.
- The purpose of the processing of the data.

You may also request access to the information submitted via the Stibo Whistleblower Scheme and request that the information is rectified, erased or blocked/made subject to restrictions in relation to processing, to the extent the information turns out to be inaccurate, misleading or in any other way processed contrary to the applicable data protection laws.

The reported individual will be notified when a report is received, and an investigation is initiated. Notification may be postponed if necessary, to ensure an effective investigation or if there are material and justified interests of Stibo Software Group which outweighs the interests of the individual being investigated. In case the actions or omissions of a reported individual have been reported under the Stibo Whistleblower Scheme and such actions and omissions are found illegal and/or in clear and serious violation of Stibo Software Group's internal guidelines or policies by the Chairman the reported individual will be subsequently informed.

Any individual may oppose processing of his/her personal data and if such objection is deemed as justified and reasonable under the circumstances, no future processing will take place.

1.9 Confidentiality and compliance with the law

Stibo Software Group and the Chairman will carry out all commercial efforts to keep the identity of the informant in question in full confidence unless the informant grants its express, prior written consent to such disclosure or unless such disclosure is required under mandatory law. If it becomes clear to the Chairman that the further processing of the information reported may be in risk of disclosing the identity of the informant, the Chairman shall seek the consent of the informant in question or, if not granted, pursue the matter at hand in a way which prevents such disclosure.

Unless the context specifically requires otherwise, all information received via the Stibo Whistleblower Scheme is treated confidentially.

Stibo Software Group will limit the number of people involved in the processing of the information to the largest extent possible. The personal data collected and processed under the Stibo Whistleblower Scheme will only be disclosed to the extent stated in this whistleblower policy. The processing of personal data under the whistleblower policy has been formally authorized by the Danish Data Protection Agency (in Danish: Datatilsynet).

1.10 Retention of data

The information received under the Stibo Whistleblower Scheme will be retained by Stibo Software Group only as long as the data is necessary for Stibo Software Group's processing of such data for the purposes of the Stibo Whistleblower Scheme. In the event that the information is dismissed as being unfounded or outside the scope of the whistleblower policy, the information will be immediately deleted.

In case the information is reported to the police or other relevant authorities, the information will be deleted immediately upon termination of the case with such authorities. In case the information is not handed over to the police or other relevant authorities, the information will be deleted. Furthermore, information will be deleted in case the information has not been handed over to the

police or other relevant authorities within 2 months after the termination of the investigation of the reported claims.

In the event that Stibo Software Group on the basis of information received by way of the Stibo Whistleblower Scheme initiates employment sanctions against the employee(s) who are the subject(s) of the report, the information in question will be retained for a period of 5 years at the personal record of the employee in question, unless there are specific legitimate reasons for a longer retention period, such as legal proceedings or similar. After such period, the information will be deleted. In case of termination of the employee, the information is kept for the 5-year period following the termination.

If you have any questions regarding confidentiality or retention of data, you are welcome to contact Stibo Systems' Legal Department.

1.11 Various

For the avoidance of doubt, it is hereby emphasized that you may only use the Stibo Whistleblower Scheme for the purposes mentioned under section 2 and to the extent specified in this whistleblower policy. Gross or repeated abuse of the Stibo Whistleblower Scheme, such as use for harassment purposes, will not be tolerated and may lead to disciplinary sanctions. If you have any questions regarding the whistleblower policy, or if you wish to exercise your rights as described under section 8, please contact Stibo Systems' Legal Department.