



GUIDELINES TO NETCOMPANY'S WHISTLEBLOWING SYSTEM
NETCOMPANY GROUP A/S

TABLE OF CONTENTS

1	INTRODUCTION	3
2	PURPOSE	3
3	WHO IS TO USE THE SYSTEM?	3
4	WHAT IS TO BE REPORTED THROUGH THE SYSTEM?	3
5	HOW DOES REPORTING THROUGH THE SYSTEM WORK?	4
6	ANONYMOUS REPORTING?	4
7	INVESTIGATION OF A REPORT	4
8	PROTECTION OF EMPLOYEES	5
9	INFORMATION TO THE EMPLOYEE REPORTED	5
10	DATA SECURITY AND DATA STORAGE	5
11	QUESTIONS	6
12	REVIEW AND AMENDMENT	6
13	PUBLICATION.....	6

GUIDELINES TO NETCOMPANY'S WHISTLEBLOWING SYSTEM

NETCOMPANY GROUP A/S

(CVR-no. 39 48 89 14)

1 INTRODUCTION

1.1 These guidelines describe why Netcompany Group A/S, CVR no. 39 48 89 14 (the "Company") has implemented a whistleblowing system, how it works and the issues that the users may report through the system.

2 PURPOSE

2.1 The purpose of these guidelines is to provide the groups of individuals below with a voluntary alternative for the reporting of serious offences in addition to the ordinary routes of communication.

3 WHO IS TO USE THE SYSTEM?

3.1 The system may be used by persons related to the Company, such as employees of the Company, members of the Executive Management and Board of Directors, auditors, lawyers, suppliers and other business partners of the Company.

3.2 The system may only be used for the reporting of persons associated with the Company, for instance employees, members of the Executive Management and Board of Directors, auditors, suppliers and legal advisors.

4 WHAT IS TO BE REPORTED THROUGH THE SYSTEM?

4.1 The system may only be used for the reporting of serious offences. Serious offences mean:

- (i) Financial crime and violation of applicable accounting rules.
- (ii) Bribery.
- (iii) Fraud.
- (iv) Forgery.
- (v) Corruption.
- (vi) Theft.
- (vii) Violation of industrial safety rules.
- (viii) Environmental pollution.
- (ix) Sexual harassment, assault and instances in which employees materially abuse access to systems in order to obtain information about co-workers or others when it is not work-related.
- (x) Violation of applicable legislation, regulations or other rules applicable the Company's business.
- (xi) Violation of internal rules provided that:
 - the violation may lead to serious, recurring security risks;
 - the violation may lead to serious financial risks;
 - the violation may lead to regulatory measures;
 - the violation may lead to a serious qualification from the auditor; or
 - the violation may seriously damage the Company's relations with employees or external parties.

- 4.2 Offences that may not be reported through the system must be reported through the usual routes of communication. This includes minor offences as for instance problems of co-operation, bullying, violation of the Company's internal guidelines about smoking, e-mails, internet, alcohol etc.
- 4.3 A report can be filed through the system when the individual knows about the issue and when the individual is suspicious of the issue.
- 4.4 When an individual files a report, the individual must keep to the facts and avoid speculation and making opinions about the issue in question.
- 4.5 The individual is requested to state the following (to the extent the individual knows or assumes it):
- (i) a description of the issue;
 - (ii) the person involved;
 - (iii) whether others know about the suspicion about the issue;
 - (iv) whether the management knows about the issue;
 - (v) whether documents exist that support the issue;
 - (vi) whether and when further information may be found about the issue;
 - (vii) whether how long the issue has existed; and
 - (viii) whether the individual knows about any attempts to hide the offence.
- 4.6 The more information that the individual provides the better the possibility of uncovering the offence.
- 4.7 It is not possible to make a further investigation of a report if the report is not specified or if it only contains very wide allegations without any specifications.

5 HOW DOES REPORTING THROUGH THE SYSTEM WORK?

- 5.1 All individuals who observe a serious offence or suspect such offence may file a report through the system. The system is a voluntary alternative to the company's ordinary routes of communication.
- 5.2 Reporting through the system may be made by means of www.whistleblower.plesner.com

6 ANONYMOUS REPORTING?

- 6.1 The Company encourages the reporting individual to state his or her name so that the Company may ask the individual further questions and subsequently inform the individual about the further course of the investigation.
- 6.2 However, it is possible to file an anonymous report. The reporting employee must be aware that anonymity can make it difficult to investigate the issue.

7 INVESTIGATION OF A REPORT

- 7.1 The Company will treat all reports as confidential.
- 7.2 When a report is filed, Plesner Advokatpartnerselskab ("Plesner") will screen the e-mail in order to ensure that it is a report that falls within the scope of the whistleblowing system.
- 7.3 If the report is about an issue that is not considered to be manifestly unfounded but that falls outside the scope of the system, the reporting individual will be requested to make an inquiry through the Company's ordinary routes of communication (for instance the employee's immediate superior, the human resources department etc). If the report is anonymous, Plesner will forward it to the Company's human resources department in Denmark.
- 7.4 If the report is considered to be manifestly unfounded, it will be deleted immediately and the Company will not be informed about the report.

- 7.5 If the report is considered to fall within the scope of the system, Plesner will forward the report to the chairman of the Audit Committee who will investigate the report. If the report concerns the chairman of the Audit Committee, Plesner will forward the report to the chairman of the Board of Directors.
- 7.6 Plesner will send quarterly lists of reports filed through the Company's whistleblowing system to the chairman of the Audit Committee.
- 7.7 In addition, the individual whom the report is about will be informed. The information will be given by Group HR.
- 7.8 Depending on the scope of the report, individuals of the organisation may become part of the investigation team and consequently obtain access to parts of or the entire report.
- 7.9 Information submitted in connection with a report will only be shared with the persons who need the information. Parts of or all the information of the report may be disclosed in the following circumstances:
- (i) In connection with interviews with "witnesses".
 - (ii) If it is required under the law or in connection with legal proceedings.
 - (iii) When information is disclosed to the employee reported in compliance with the rules of the Danish Data Protection Act on right of access.

8 PROTECTION OF EMPLOYEES

- 8.1 If in good faith an employee files a report through the system that may later turn out to be groundless, it will not have any negative consequences for the employee neither in terms of his/her employment nor promotion.
- 8.2 The Company does not accept that employees deliberately file false reports and it may have employment law repercussions if an employee deliberately files a false report about another employee through the system.
- 8.3 The identity of the reporting employee will as a starting point not be disclosed to the employee being reported. However, the identity of the employee will be disclosed if it may turn out that the reporting employee has filed a deliberately false report.
- 8.4 The identity could also be disclosed in any subsequent legal proceedings concerning the situation reported.

9 INFORMATION TO THE EMPLOYEE REPORTED

- 9.1 If an individual is reported through the system, the individual will be informed as soon as possible after a preliminary investigation has taken place and all relevant evidence has been secured. The individual will for instance be informed about:
- (i) The identity of the person/group responsible for the investigation of the report.
 - (ii) A description of the accusations.
 - (iii) The persons who have seen the report.
- 9.2 Details about the rights of reported individuals can be found in "Netcompany's Whistleblower System - Guidelines for Reported Persons" <https://www.netcompany.com/int/Whistleblower>.

10 DATA SECURITY AND DATA STORAGE

- 10.1 The Company will process the individuals' information and all information covered by a report in accordance with applicable law.
- 10.2 All reports will be stored properly and it will only be possible for relevant persons to access the reports.
- 10.3 Reports that turn out to be unfounded will be deleted immediately. If an offence is reported that falls outside the category of serious offences that may be reported through the programme, see section 3, the report will immediately be sent to the person with personnel responsibilities in charge of the person

reported and will at the same be deleted from the whistleblowing system. If the offence is reported to the police or another authority, the information will be deleted immediately after the case has been closed by the authorities in question.

- 10.4 If based on the information gathered employment law sanctions are implemented against the person reported or other reasons exist as to why it is fair and necessary to continue to store information about the employee, such information will be stored in the relevant personnel file. After resignation the information about the employee will be stored for up to 5 years.

11 QUESTIONS

- 11.1 If you have any questions regarding these guidelines, please do not hesitate to contact:

- Tine K. Boye on tkb@netcompany.com / +45 24 91 75 33

12 REVIEW AND AMENDMENT

- 12.1 The Audit Committee shall continuously review, and if relevant update, these guidelines.

13 PUBLICATION

- 13.1 These guidelines will be published on the Company's website.