



Policy on the Continia Software Whistleblower Scheme

1. Background and purpose

- 1.1 The board of directors of Continia Software A/S (the "**Company**") has adopted this policy on the Continia Software Whistleblower Scheme (the "**Policy**") in accordance with the Danish Whistleblower act and the act on Measures to Prevent Money Laundering and Financing of Terrorism art. 35-36.
- 1.2 This Policy describes the overall whistleblower principles of the Company.
- 1.3 The Company practices a high level of ethical standard in business and personal conduct. The entire management, all employees, and representatives of the Company must practice integrity in fulfilling responsibilities and comply with high moral standards and all applicable laws and company policies.
- 1.4 The Company has adopted this whistleblowing Policy to ensure access to anonymous and safe reporting of any potential violation.

The Company is committed to maintaining a culture of integrity, transparency, and accountability. This whistleblower Policy is designed to provide a mechanism for employees and stakeholders to report any concerns or suspicions of illegal, unethical, or fraudulent activities within the Company or any of the subsidiaries or projects which the Company, at any time, is a part of.

- 1.5 The whistleblower Policy includes the information and guidelines on the Continia Software Whistleblower Scheme, describing the whistleblower protection, the Whistleblower Committee, and the process for both internal and external whistleblowing.

2. Policy scope and strategic goal

The Policy applies to the Company's management, employees and representatives of the Company and it is mandatory to comply with this Policy.

The strategic goal of the Policy is to determine the overall principles for the protection of whistleblowers in the Company. These principles are implemented in operational procedures, guidelines and all relevant information on the Whistleblower platform.

3. Whistleblower risk identification

The risks associated with whistleblowing can be, but are not limited to, situations such as:



- Relevant incidents may not be reported to the management.
- A whistleblower may experience retaliation, inappropriate exposure or consequence based on reporting on relevant incidents.
- The whistleblower may not report on relevant incidents out of fear of retaliation.
- The whistleblower may report in bad faith.

4. Risk management related to the Whistleblower Scheme

- 4.1 The Company will not tolerate any violations of regulation or of the Company's policies and underlying business procedures.
- 4.2 The Whistleblower Scheme applies to every person in or interacting with the Company. That includes, but is not limited to employees, managers, board members, investors, contractors, vendors, or other people interacting with the Company.
- 4.3 The following concerns can be raised under the whistleblower scheme: (i) Breaches of EU law that fall within the scope of Directive (EU) 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law (the "Whistleblower Directive") and (ii) other serious breaches of Danish and EU law as well as other serious concerns.
- 4.4 Suspected breaches of the specific EU legal acts that fall within the scope of the Whistleblower Directive do not have to be serious. The Whistleblower Directive applies to breaches of those EU legal acts that are listed exhaustively in Part I in the annex to the Whistleblower Directive, inter alia, in the following areas:
- prevention of money laundering and terrorist financing,
 - product safety and compliance,
 - protection of the environment,
 - public health,
 - consumer protection,
 - protection of privacy and personal data, and
 - security of network and information systems.
- 4.5 Breaches affecting the financial interests of the EU and breaches relating to the internal market, including breaches of EU competition and state aid rules are also included in the scope.
- 4.6 Serious breaches of Danish and EU law and other serious concerns may also be reported, including, inter alia:
- criminal acts such as breaches of non-disclosure obligations, abuse of



funds, theft, fraudulent misrepresentation, embezzlement, fraud, and bribery,

- serious or repeated infringements of the law, including legislation on the use of force, the Danish Public Administration Act, the Danish Act on Access to Public Records and legislation intended to protect public health, provide safety in the transport sector, or protect the nature and the environment, etc.,
- sexual harassment in the workplace,
- serious person-related conflicts in the workplace, for instance serious harassment on grounds of race, political affiliation, religious belief, etc., and
- serious violations of occupational safety rules.

4.7 The Company strictly prohibits retaliation against individuals who make reports in good faith.

4.8 The protection of whistleblowers against retaliation in the whistleblower scheme covers employees, intermediaries, third parties connected to the whistleblower and companies or authorities that the whistleblower owns, work for or is otherwise professionally connected to (hereafter collectively referred to as "**employee**").

5. Protection of the whistleblower - rights

5.1 The Company shall not retaliate against any individual who reports an incident relevant for whistleblower reporting ("**Relevant Incidents**"). Any such retaliation or inappropriate exposure or consequence shall be considered a violation of the Policy and the Company's Code of Conduct.

5.2 The whistleblower scheme ensures the whistleblowers right to report anonymously. The anonymity of the whistleblower is ensured by the digital whistleblower solution the Company has implemented.

5.3 Any personal data of any individual involved will be treated confidentially in accordance with the personal data and employment legislation applicable.

5.4 If the report falls within the scope of the whistleblower scheme, the whistleblower has a right to rely on a report to seek dismissal of a case, provided that the whistleblower had reasonable grounds to believe that the reporting was necessary for revealing a breach that falls within the scope of the Danish Whistleblower Act.

5.5 If you meet the criteria for protection, you will not be deemed to have breached any statutory non-disclosure obligation and will not incur liability in that respect, provided that you had reasonable ground to believe that the report was necessary to disclose a breach falling within the scope of the Danish Whistleblower Act. Nor will you incur liability for getting access to the reported disclosures, provided that such access did not constitute a self-standing criminal offence.



6. Protection of the person concerned - rights

- 6.1 The Company ensures that the identity of the person concerned is protected in connection with handling the report and that the person concerned has access to an effective defense, including, among other things, by recording reports.

7. Roles and responsibilities

- 7.1 The Company has established a Whistleblower Committee to handle whistleblower reports.
- 7.2 The Whistleblower Committees members responsibilities and procedures are described in the Continia Software Whistleblower Scheme, which ensures fair and effective handling of all whistleblower reports in accordance with the Policy.
- 7.3 Upon receipt of a whistleblower report, the whistleblower committee will promptly investigate the allegations in a fair, objective, and confidential manner.
- 7.4 The Company will maintain records of all whistleblower reports and related investigations in a secure and confidential manner, in compliance with applicable data protection regulations. The retention period will be determined based on legal requirements and the nature of the reported concerns.
- 7.5 The Whistleblower Committee will provide a written acknowledgement to the whistleblower as specified in the relevant guideline in the Whistleblower scheme within the specified timeframe, outlining the steps taken and the expected timeline for the investigation. Should the reported matter fall outside the scope of the Whistleblower regulations the committee will process the reported matter in the same manner as any reported issue and return a documented report to the Whistleblower within the same timeframe as any reported issue explaining why it falls without the scope of the regulations.
- 7.6 Upon completion of the investigation, the Whistleblower Committee will communicate the findings to the whistleblower, to the extent permitted by law, while respecting the rights of all parties involved.
- 7.7 The members of the Whistleblower Committee have a duty of confidentiality in respect of all disclosures made in whistleblower reports. The duty of confidentiality also applies to other members of staff who assist with following up on reports and, in doing so, receive information that must be treated confidentially.
- 7.8 As the main rule, information about the whistleblower's identity and other information from which the whistleblower's identity can be deduced, directly or indirectly, may not be disclosed without your explicit consent to anyone beyond the Whistleblower



Committee.

8. Responsibilities of the CEO and the employees

8.1 The Company's CEO has the overall responsibility for the whistleblower scheme and is supported by the Whistleblower Committee.

8.2 All board members and employees of the Company must report any concerns or suspicions of illegal, unethical, or fraudulent activities within the Company in accordance with the active guidelines, Code of conduct and regulations relevant to the Continia Software Whistleblower Scheme.

8.3 All management members and employees of the Company must comply with the Policy as well as underlying guidelines and standard operating procedures.

9. Reporting and sanctions

9.1 All the Company's employees, regardless of their job description and function, must report situations that involve or could potentially involve any violations of regulation or of the Company's framework of policies, guidelines and operating procedures.

9.2 The Company will not subject the whistleblower to any unfavorable treatment or unfavorable consequences as a result of the reporting.

9.3 The Company considers any breach of the Policy or of any procedures and measures established based on the Policy, including applicable guidelines, a serious matter. Such breach will result in a warning, and serious or repeated breaches may result in dismissal or summary dismissal.

9.4 The Whistleblower Committee will report on whistleblower reports received to the management and the board of directors.

10. External whistleblowing

10.1 The whistleblower is free to choose whether to report the concerns under the Company's internal whistleblower scheme or under any relevant external whistleblower scheme or under both. However, we encourage the whistleblower to use the Company's internal whistleblower scheme if the breach can be effectively addressed internally and if you consider the risk of retaliation to be non-existent.

10.2 The procedure for reporting to the Danish Data Protection Agency's external whistleblower scheme can be found here: <https://whistleblower.dk/>.

11. Review and update



- 11.1 Any amendments or addendums to the Policy must be adopted by the board of directors.
- 11.2 The committee will be responsible for preparing draft amendments or addendums to the Policy. Should the Policy no longer be appropriate or should laws, or rules promulgated thereunder, so require.
- 11.3 The Policy must be reviewed at least once a year.

12. Document history

Version	Changes	Responsible For changes	Document approved by	Date of approval
Version 1	New policy	Committee	Bord of directors	01.12.2023
Version 1.1	Additional information added & review	Committee	Bord of directors	18.12.2024