WHISTLEBLOWER POLICY CONCERNING

AARHUS UNIVERSITY'S WHISTLEBLOWER SCHEME

10 December 2021

WHISTLEBLOWER POLICY

1 INTRODUCTION AND PURPOSE

1.1 This whistleblower policy describes the purpose of the Aarhus University (hereinafter referred to as the "**University**") whistleblower scheme (hereinafter referred to as the "**Scheme**"), how the Scheme works, who can use the Scheme and what can be reported through the Scheme.

1.2 The aim of the Scheme is to ensure that a whistleblower, as defined in this whistleblower policy, is able to report breaches or potential breaches covered by the Danish Act on whistleblower protection (hereinafter referred to as the "**Whistleblower Act**") in a swift and confidential manner, through a special, independent and separate channel, thereby ensuring that an impartial and independent whistleblower unit decides on the action to be taken.

2 WHO CAN USE THE SCHEME?

2.1 The Scheme may be used by persons who report information about breaches that they have acquired in connection with their work-related activities, and who belong to any of the following groups of persons (hereinafter referred to as "**whistleblower**"):

(ii) Employees.

(iii) Self-employed persons.

(iv) Members of the senior management team and the board.

(v) Volunteers.

(vi) Paid or unpaid interns.

(vii) Persons working under the supervision and direction of contractors, subcontractors and suppliers.

(viii) Persons who report or publicly disclose information acquired in a work-based relationship that has since ended.

(ix) Persons whose work-based relationship is yet to begin and who report information on breaches that they have obtained during the recruitment process or other pre-contractual negotiations.

2.2 Persons covered by section 9.1.5 may also report information under the Scheme (for example a facilitator who assists the whistleblower in the reporting process in a work-related context).

2.3 Persons who are not part of the group of persons described in section 2.1 or 9.1.5 cannot report information through the Scheme, but instead should report through the usual communication channels. If conditions are otherwise fulfilled, reporting may be through the Danish Data Protection Agency's external whistleblower scheme as described in section 10.

3 WHAT MAY BE REPORTED THROUGH THE SCHEME?

3.1 The Scheme covers reports on serious breaches of law or other serious wrongdoings (see section 3.4 (i)) or breaches of EU law within the scope of the Whistleblowing Directive (see section 3.4 (ii)).

3.2 "Breaches" means acts or omissions that

a) are unlawful, or constitute a serious breach or another serious wrongdoing covered by section 3.4, or

b) defeat the object or the purpose of the rules falling within section 3.4.

3.3 It is possible to report any information, including reasonable suspicion, about actual or potential breaches or serious wrongdoings covered by section 3.4, which occurred or are very likely to occur at the University, and about attempts to conceal such breaches.

3.4 The report must concern breaches or potential breaches covered by the Whistleblower Act and defined as acts or omissions that:

(i) constitute a serious breach or other serious wrongdoing, such as:

- Breach of confidentiality, if applicable
- Misuse of funds
- Theft
- Fraud
- Embezzlement
- Deceit
- Bribery
- Work safety breaches
- Any form of sexual harassment
- Serious harassment, e.g. bullying, violence and harassment due to race or political or religious affiliation.
- Serious or repeated breaches of the principles of administrative law, including the inquisitorial principle, requirements for objectivity, the misuse of powers doctrine and proportionality.
- Deliberately misleading information

(ii) are unlawful under EU law within a number of specific areas, including:

- Public calls for tender
- Money laundering
- Product safety and compliance
- Transport safety
- Food and feed safety
- Animal health and welfare
- Environmental protection
- Public health
- Consumer protection
- Protection of privacy and personal data
- Network and information system security

In this connection, reference is made to this list, containing legislation covered by the Scheme.

3.5 The Scheme may only be used to report breaches or potential breaches of the regulation mentioned in section 3.4, which have occurred or will most likely occur in the University's organisation, including breaches by employees, members of the senior management team or the board. By stating that reports may concern wrongdoings committed by the University, it should be noted that the aforementioned wrongdoings may be reported even if they cannot be attributed to a single person, but are due to a fundamental system error at the University.

3.6 Offences that are not covered by the Scheme must be reported through the usual communication channels. If conditions are otherwise fulfilled, reporting may be through the Danish Data Protection Agency's external whistleblower scheme as described in section 10.

3.7 Note that the whistleblower scheme does not restrict the freedom of speech of public sector employees, and that the freedom of speech and whistleblower rights laid down in relevant regulations still exist.

4 CONTENT OF THE REPORT

4.1 For the sake of further investigation of the report, including establishing the nature of the offence, it is important that the whistle-blower describes the offence in as much detail as possible. Thus, it is not possible to conduct a more detailed investigation of a report if the report is vague or if it only contains very general accusations without further clarification.

4.2 Consequently, the whistleblower should, as far as possible, include the following information in the report:

- a description of the wrongdoing,
- who is involved,
- whether others are aware of the suspected wrongdoing,
- whether management is aware of the wrongdoing,
- whether documents exist that provide evidence of the wrongdoing,
- whether additional information about the wrongdoing is available, and if so where,
- how long the wrongdoing has been going on, and
- whether the whistleblower is aware of any attempts to conceal the offence.

4.3 Manifestly unfounded reports will not be subject to further investigation.

5 HOW CAN REPORTING TAKE PLACE, AND WHO SHOULD THE REPORT BE SUBMITTED TO?

5.1 The university has set up a whistleblower unit to

(a) receive reports and be in contact with the whistleblower,

(b) follow up on reports, and

(c) give feedback to the whistleblower.

5.2 The whistleblower unit in charge of the tasks mentioned in section 5.1 consists of two attorneys-at-law from Plesner Advokatpartnerselskab, a Danish law firm (hereinafter referred to as "**Plesner**"), and an impartial group of persons from the University.

5.3 Written reports are to be submitted through the Plesner whistleblower scheme. A link to the scheme can be found on the University's website: https://whistleblower.plesner.com/direct.aspx?c=AarhusUniversitet

5.4 Written reports are received by two attorneys-at-law at Plesner. Plesner makes an assessment of the impartiality of the persons in the whistleblower unit to determine who is able to deal with the report, and then forwards the report to these persons (hereinafter referred to as "**Case Officers**") at the University. Prior to forwarding the report, Plesner assesses whether the report falls within the scope of the Scheme.

5.5 Only written reports can be made under the Scheme.

5.6 The whistleblower unit treats all written reports confidentially.

5.7 The Case Officers appointed to receive and follow up on reports have a duty of confidentiality with regard to information included in the report. See, however, section 8.3 and sections 9.1.7-9.1.9.

6 ANONYMITY

6.1 The University recommends that whistleblowers state their name when they report, so that the Case Workers can contact them to ask clarifying questions and keep them updated on how the investigation progresses. However, anonymous communication between Plesner and a whistleblower is also possible if the whistleblower wants to remain anonymous (see sections 6.4 and 6.5).

6.2 If the whistleblower prefers anonymous reporting, it is recommended that the whistleblower use a private PC or a PC located at a public library, for example, in order to ensure full anonymity.

6.3 Plesner provides a communication module that enables the whistleblower to communicate with Plesner and provide additional information about the reported breach, and Plesner will then pass on this information to the Case Officers.

6.4 If the whistleblower prefers to report anonymously, it is possible for the whistleblower to communicate anonymously with Plesner via the communication module. The whistleblower may thus provide additional information to Plesner via the communication module and remain anonymous. In connection with the reporting, a single-use code will be generated in order to guarantee anonymity. This code cannot be recreated. Therefore, it is **important** that the whistleblower saves the code and remembers to log on to the communication module in order to communicate with the whistleblower unit.

6.5 The communication module is accessed via the above-mentioned link to the Scheme (see section 5.3), from where the whistleblower can log on to the communication module. If the whistleblower prefers to be anonymous, it is important that the whistleblower regularly accesses the communication module to check whether Plesner has asked questions. If the whistleblower is anonymous, Plesner is not able to contact the whistleblower in any other way nor make the whistleblower aware that additional questions have been asked, etc.

6.6 The identity of the whistleblower enjoys special protection in pursuance of the Whistleblower Act. Reports covered by the scope of the Whistleblower Act are not subject to the right of access to documents under the Access to Public Administration Files Act, for example. Any person who is a party to a case that the report concerns or has given rise to, has no right to be informed about the whistleblower's identity or to information that may identify the whistleblower.

7 INFORMATION FOR WHISTLEBLOWERS

7.1 The whistleblower will receive:

- a confirmation of receipt of the report from Plesner within seven days, and
- feedback from the University as soon as possible, generally within three months of confirmation of receipt of the report.

7.2 Feedback is defined as information about the action taken by the University to assess the correctness of the claims made in the report, and, where relevant, to address the reported breach. The feedback provided by the whistleblower unit must always comply with relevant legislation, including personal data protection regulations and sections 25 and 26 of the Whistleblower Act concerning confidentiality and disclosure. This may result in restrictions on the feedback received by the whistleblower.

7.3 Depending on the situation, it may be necessary to extend the timeframe for feedback in light of the specific circumstances of the case, in particular the nature and complexity of the reporting, which may call for a prolonged investigation. In this case, the whistleblower will be notified.

8 INFORMATION FOR AND PROTECTION OF THE PERSON CONCERNED

8.1 When a preliminary investigation, including an initial assessment of the scope and processing of the case, has been carried out, and all relevant evidence has been secured, the person concerned, i.e. the person reported under the Scheme, will be notified about:

- the identity of the Case Officer(s) responsible for investigating the report, and
- the wrongdoings that the report concerns.

8.2 Under the Whistleblower Act, the person concerned is entitled to protection of their identity during the processing of the case and to an effective defence. These rights cannot be derogated from by any agreement to the detriment of the person concerned.

8.3 In certain circumstances, the person concerned will have the right to access information about the identity of the whistleblower, if this is necessary in order for the person concerned to be able to exercise the right to an effective defence (see 9.1.7).

8.4 The University otherwise observes the rights of the person concerned stipulated in the General Data Protection Regulation. Furthermore, reference is made to the University's privacy policy for the whistleblowing scheme, which is available on the website of Aarhus University, and provides additional information on processing of personal data and the rights of data subjects.

9 PROTECTION OF WHISTLEBLOWERS

9.1 Terms and conditions for protection of whistleblowers

9.1.1 Pursuant to the Whistleblower Act, whistleblowers enjoy protection against retaliation if the whistleblower has reported breaches under the Scheme. Protection is only granted if all of the following conditions are met:

- The person reporting meets the conditions for being a whistleblower (see section 2).
- The whistleblower had reasonable reason to assume that the information reported was correct at the time of the report.
- The information reported falls under the scope of the Whistleblower Act (see section 3.4).

9.1.2 Any person reporting under the Scheme who does not meet the conditions stated in section 9.1.1 enjoys no protection under the Whistleblower Act. If the person enjoys no protection, the person will be given the opportunity to withdraw their report unless it concerns circumstances that necessitate a more detailed investigation of the matter by the University.

9.1.3 "Retaliation" is defined as unfavourable treatment or unfavourable consequences in response to a report. This includes suspension, dismissal, demotion, etc.

9.1.4 If the whistleblower reports in bad faith, knowing that the reported information is incorrect, the whistleblower enjoys no protection against retaliation. Depending on the circumstances, the whistleblower may be punished by a fine if false claims have been reported intentionally. Furthermore, if the whistleblower is employed at the University, false reporting may also have consequences for the employment relationship, including that the whistleblower may be dismissed summarily.

9.1.5 In addition to the group of persons mentioned in section 2.1, the protection described in this section (section 9) also includes the following persons:

1) Facilitators (any natural person who assists the whistleblower in the reporting process in a work-related context).
2) Third parties who are connected with the whistleblower and who could suffer retaliation in a work-related context (such as a colleague).
3) Businesses or authorities that the whistleblower owns or works for or is otherwise connected with in a work-related context (such as a business owned by the whistleblower).

9.1.6 Information about the whistleblower's identity or other information that may directly or indirectly identify the whistleblower, will only ´be disclosed to parties other than the whistleblower unit after obtaining the whistleblower's express consent and after the recipient of such information has signed a declaration of confidentiality.

9.1.7 However, information about the whistleblower's identity may, without consent, be disclosed to other public authorities if the purpose of such disclosure is to prevent breaches (e.g. a criminal act that has not yet taken place), or to secure the right to defence of the persons concerned. If the whistleblower's identity is disclosed without consent, the whistleblower will be informed hereof, including the reason for the

disclosure, unless such notification will jeopardise related investigations or legal proceedings. See section 8.3 for more details on disclosure of the whistleblower's identity.

9.1.8 The whistleblower's identity may also be disclosed in connection with any legal proceedings concerning the reported wrongdoing.

9.1.9 Other information from the report, i.e. information that does not reveal the whistleblower's identity, will only be disclosed to persons outside the whistleblower unit (assistants) as part of an investigation of or follow-up on a report. Before receiving information from the report, the assistant must sign a declaration of confidentiality. Information may also be disclosed in order to prevent a potential breach of the conditions stated in section 3.4.

10 EXTERNAL WHISTLEBLOWER SCHEMES

10.1 The whistleblower can choose freely between reporting under the Scheme or the Danish Data Protection Agency's external whistleblower scheme, which can be accessed here: https://whistleblower.dk/indberet.

11 DATA SECURITY AND DATA STORAGE

11.1 The University registers all reports received through the Scheme. Registration will be in accordance with the duty of confidentiality laid down in the Whistleblower Act. The University will store a report for as long as it is necessary and proportionate to comply with the requirements stipulated under Danish law.

11.2 The University and Plesner process all information reported through the Scheme, including information about persons reported through the Scheme, in accordance with the legislation in force at any time.

11.3 All reports will be stored securely, and it will only be possible for relevant persons in the whistleblower unit or assistants who have signed a declaration of confidentiality to access the information.

11.4 If a report falls outside the scope of the Scheme, the whistleblower will, as a general rule, be given the opportunity to withdraw the report, unless the report concerns circumstances that necessitate further action by the University. In any case, the report submitted under the Scheme will be closed. Any further processing of the report will be carried out under the auspices of the relevant unit at the University.

11.5 As a general rule, reports are deleted from the Scheme 45 days after the University has completed the processing, unless the University has a legitimate reason for continued storage, for example if storage is required according to other legislation, or if there is reason to believe that the report may be corroborated by subsequent reports on the same wrongdoing. The University also stores reports, other case processing steps and investigations in the University's ESDH system in accordance with the legislation in force at any time, including legislation on archiving and deletion.

11.6 If the matter is reported to the police or another authority, the report will be closed in the Scheme immediately after the case has been closed by the relevant authorities.

11.7 If, on the basis of the data collected, a disciplinary sanction is imposed on the person concerned, or if there are other reasons why continued storage of information about the person concerned is relevant and necessary, information concerning an employee must be stored in the employee's personal file.

11.8 The information is otherwise stored in accordance with the University's deletion policy.

12 PUBLICATION

12.1 Once a year, the University publishes statistics for the use of the whistleblower scheme on the University website.

13 QUESTIONS

13.1 If you have any questions about this whistleblower policy, please contact legal@au.dk.

14 UPDATES

14.1 This whistleblower policy was most recently updated: *December* 2021