

PRIVACY POLICY FOR WHISTLEBLOWER SCHEME

AARHUS UNIVERSITY

This privacy policy describes how Aarhus University ("the **University**", "**we**" or "**us**") processes personal data in connection with reports to the University's whistleblower scheme.

Below is a detailed description of how the processing of personal data takes place, and your rights if another person makes a report about you to the whistleblower scheme. Furthermore, there is a detailed description of your rights if you use the whistleblower scheme to make a report about another person.

For details about who can make a report and who a report may concern, see the University's whistleblower policy.

This privacy policy only applies to the processing and investigation of reports under the whistleblower scheme. Consequently, in relation to employees, the policy should be seen in the context of other relevant policies and procedures at the University.

1 DATA CONTROLLER

The legal entity responsible for processing your personal data is:

Aarhus University

CVR no.: 31119103

Nordre Ringgade 1

DK-8000 Aarhus C

Email: au@au.dk

2 DESCRIPTION OF PROCESSING

2.1 Statutory whistleblower scheme under the Danish Whistleblower Act

Below is a description of how the University processes information about the person who a report concerns ("**the person concerned**") as well as the person making the report ("**the whistleblower**") in connection with reports under the University's whistleblower scheme set up in accordance with the Danish Whistleblower Act.

Purpose	Categories of personal data	Basis for processing	Recipients	Storage
<p>#1 Processing and investigation of reports covered by the University's whistleblower scheme concerning:</p> <ul style="list-style-type: none"> The person concerned 	<p>We may process the following categories of personal data about you:</p> <p><u>Ordinary personal data:</u></p> <ul style="list-style-type: none"> Name, email address, telephone number, Other information included in the report. <p><u>Sensitive data</u>, including data concerning sex life, may be included in the processing.</p> <p><u>Data about offences or possible offences</u> may also be included in the processing.</p>	<p>We process your personal data based on the following basis for processing.</p> <ul style="list-style-type: none"> Section 22 of the Whistleblower Act: Necessary for the University to process reports received as part of the University's whistleblower scheme set up in accordance with the Whistleblower Act, see <ul style="list-style-type: none"> point (c) of Article 6(1) of the GDPR: Necessary for compliance with a legal obligation to which the University is subject in accordance with section 9 of the Whistleblower Act. Point (e) of Article 6(1) of the GDPR: Necessary for the performance of a task carried out in the public interest Point (g) of Article 9(2) of the GDPR: Processing is necessary for reasons of substantial public interest in accordance with section 9 of the Whistleblower Act. Section 8(5) of the Danish Data Protection Act, see section 7(4) of the same Act, see point (g) of Article 9(2) of the GDPR. 	<p>We may disclose your personal data to:</p> <ul style="list-style-type: none"> Plesner Advokatpartnerselskab (Danish law firm) IT suppliers External advisers The police Public authorities such as the Danish Financial Supervisory Authority, the Danish Data Protection Agency or relevant tax authorities 	<p>We will store personal data for as long as this is necessary for the purposes described.</p> <ul style="list-style-type: none"> The data will be stored for as long as the investigation is ongoing. The storage period depends on the outcome of the investigation. As a general rule, reports will be deleted from the IT solution at Plesner 45 days after the University has completed the processing, unless the University has a legitimate reason for continued storage. Reports that fall outside the scope of the Scheme, but which do not otherwise appear to be unfounded, will be passed on to the Rector's Office for an assessment of who can process the case in accordance with the University's relevant policies and procedures. Reports that turn out to be unfounded will be completed immediately in the Scheme and deleted from the IT solution at Plesner within 45 days after ascertaining that the report was considered to be unfounded. If a matter is reported to the police or to another authority, the data will be stored at least for as long as the investigation is ongoing at the police/authority.
<p>Sources</p> <p>We may collect data from the following sources:</p> <ul style="list-style-type: none"> Plesner Advokatpartnerselskab (Danish law firm) Employees at the University Self-employed persons. Members of the University senior management team or board Volunteers Paid and/or unpaid interns. Persons working under the supervision and direction of contractors, suppliers and sub-suppliers. Persons who report information acquired in a work-based relationship that has since ended. Persons whose work-based relationship is yet to begin and who report information on breaches that they have obtained during the 				

<p>recruitment process or other pre-contractual negotiations.</p> <ul style="list-style-type: none"> Any other persons who may report through the scheme. 				<ul style="list-style-type: none"> The information is otherwise stored in accordance with the University's deletion policy.
Purpose	Categories of personal data	Basis for processing	Recipients	Storage
<p>#2 Processing and investigation of reports covered by the University's whistleblower scheme concerning:</p> <ul style="list-style-type: none"> The whistleblower <p>If there is a suspicion that a report is knowingly false, this purpose also includes an investigation of the reporting person in such situations.</p>	<p>We may process the following categories of personal data about you, provided that your report is not anonymous.</p> <p><u>Ordinary personal data:</u></p> <ul style="list-style-type: none"> Name, email address, telephone number, The content of your report 	<p>We process your personal data based on the following basis for processing</p> <ul style="list-style-type: none"> Section 22 of the Whistleblower Act: Necessary for the University to process reports received as part of the University's whistleblower scheme set up in accordance with the Whistleblower Act, see <ul style="list-style-type: none"> point (c) of Article 6(1) of the GDPR: Necessary for compliance with a legal obligation to which the University is subject in accordance 	<p>We may disclose your personal data to:</p> <ul style="list-style-type: none"> Plesner Advokatpartnerse Iskab (Danish law firm) IT suppliers External advisers The police Public authorities such as the Danish Financial Supervisory 	<p>We will store personal data for as long as this is necessary for the purposes described.</p> <ul style="list-style-type: none"> The data will be stored for as long as the investigation is ongoing. The storage period depends on the outcome of the investigation. As a general rule, reports will be deleted from the IT solution at Plesner 45 days after the University has completed the processing, unless the University has a legitimate reason for continued storage. Reports that fall outside the scope of the Scheme, but which do not otherwise
Sources	<p>As a general rule, we do not process sensitive data about</p>			

<p>We may collect data from the following sources:</p> <ul style="list-style-type: none"> • Plesner Advokatpartnerselskab (Danish law firm) • You as the whistleblower 	<p>you when dealing with the report itself – unless you choose to provide such information about yourself.</p> <p>Information about offences or possible offences may, however, form part of the processing if there is a suspicion that a report is knowingly false.</p>	<p>with section 9 of the Whistleblower Act.</p> <ul style="list-style-type: none"> - Point (e) of Article 6(1) of the GDPR: Necessary for the performance of a task carried out in the public interest - Point (g) of Article 9(2) of the GDPR: Processing is necessary for reasons of substantial public interest in accordance with section 9 of the Whistleblower Act. - Section 8(5) of the Danish Data Protection Act, see section 7(4) of the same Act, see point (g) of Article 9(2) of the GDPR. 	<p>Authority, the Danish Data Protection Agency or relevant tax authorities</p>	<p>appear to be unfounded, will be passed on to the Rector's Office for an assessment of who can process the case in accordance with the University's relevant policies and procedures.</p> <ul style="list-style-type: none"> • Reports that turn out to be unfounded will be completed immediately in the Scheme and deleted from the IT solution at Plesner within 45 days after ascertaining that the report was considered to be unfounded. • If a matter is reported to the police or to another authority, the data will be stored at least for as long as the investigation is ongoing at the police/authority. • The information is otherwise stored in accordance with the University's deletion policy.
--	---	---	---	---

3 INFORMATION TO THE PERSON CONCERNED AND RECTIFICATION

If a report is made through the whistleblower scheme that concerns you, you will be notified as soon as possible after a preliminary investigation has been conducted and all relevant evidence has been secured. In this connection, you will receive information about:

- The identity of the person(s) responsible for investigating the report
- A description of the contents of the report

Notification to you is in accordance with the duty of confidentiality of the whistleblower unit, cf. Article 25 of the Whistleblower Act. Therefore, an exception to the duty of disclosure will be made to the extent that the terms in Article 14(5) of the General Data Protection Regulation or Article 22 of the Danish Data Protection Act are met.

As stated in the section below on your general rights, you have the right to request access to the report made about you. However, pursuant to the regulations of the Whistleblower Act, there may be restrictions on your right of access.

You also have the right to request that data in the report be rectified if you believe such data to be inaccurate, misleading or incomplete. If your request for rectification cannot be complied with, the data will be supplemented with your comments.

4 CONSEQUENCES OF THE PROCESSING

Reports to the whistleblower scheme and investigations of reports to the whistleblower scheme may have significant consequences for you as the person concerned, as reports concern breaches or suspicion of illegal acts, as the scheme is defined in the separate guidelines for the scheme.

Similarly, reports to the whistleblower scheme may have significant consequences for you as the whistleblower in the event that the report is intentionally false. Such cases may be prosecuted, among other things.

5 TRANSFER TO NON-EU/EEA COUNTRIES

Personal data regarding you as the person concerned or you as the whistleblower will not be transferred to non-EU/EEA countries.

6 GENERAL RIGHTS

As the person concerned or the whistleblower you have the following rights:

- You have the right to request insight, rectification or deletion of your personal data.
- You also have the right to oppose the processing of your personal data and have the processing of your personal data limited.
- You have the right to receive the personal data that you provided yourself in a structured, commonly used and machine-readable format (data portability).
- You may lodge an appeal to the Danish Data Protection Agency at any time. You can read about your rights and opportunities to appeal on the Data Protection Agency website www.datatilsynet.dk. The Danish Data Protection Agency may be contacted by telephone: +45 33193200 or email: dt@datatilsynet.dk.

Furthermore, you have a right to object to our processing of your personal data:

- If our processing of your personal data is based on point (e) of Article 6(1) (public-sector interest or official authority), or point (f) of Article 6(1) (balancing of interests) (see under basis for processing in the table above), you have the right to object to such processing at any time for reasons that might concern your specific situation.

These rights may be subject to conditions or limitations. For example, you are not assured a right to have information about you deleted in the specific case – this depends on the specific circumstances related to the processing activities.

You can exercise your rights by contacting the University's data protection officer/DPO, Søren Broberg Nielsen, dpo@au.dk, + 45 87 15 31 98.

7 IT POLICY

For University employees, see also the University's [Information security policy](#) and [Email policy](#), with information about the University's policies on IT and emails.

8 QUESTIONS

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

Last updated: March 2022