WHISTLE-BLOWING
STANDARD OPERATING PROCEDURE AND POLICY

1. Introduction and purpose

1.1 This standard operating procedure and policy (the "Procedure") for AW Group describes the procedure for reporting of serious offences as defined in Section 2 through AW Group's whistle-blower system.

1.2 The purpose of the Procedure is to ensure that persons who may use the service know the procedure for reporting suspicions through AW Group's various reporting channels.

1.3 The aims of AW Group's whistle-blower system and this policy are:

- To uphold AW Groups Code of Conduct by encouraging staff to report suspected serious wrongdoing as soon as possible in the knowledge that their concerns will be taken seriously and investigated as appropriate and that their confidentiality will be respected.
- To provide staff and other individuals with guidance as to how to raise those concerns.
- To reassure staff that they should be able to raise genuine concerns without fear of reprisals, even if they turn out to be mistaken.
- To set out the procedure for handling reports made by whistle-blowers through AW Group's whistle-blower system.

2. Scope

2.1 The whistle-blowing system may be used by all employees, directors, members of the board of directors of AW Group, clients, suppliers and other individuals to report serious offences or suspected serious offences.

2.2 AW Group encourages that serious offences are reported by use of AW Group's whistle-blowing hotline Speak Up. However, it is emphasized that the system is a voluntary alternative to the ordinary communication channels, e.g., local management, local People and Performance responsible, group management or group legal.

2.3 AW Group encourages its staff and other individuals to use the whistle-blower system and to protect all whistle-blowers who makes a report in a good faith. Such persons will not be subjected to any adverse treatment or adverse consequence.

2.4 The whistle-blower system is not an emergency hotline. Any issues that constitute immediate threats i.e. where there is a threat to health, life etc. should be reported through the ordinary emergency channels.

2.5 Types of serious misconduct:

- Bribery
- Fraud
- Forgery
- Corruption
- Theft
- Conflict of interest
- Discrimination
- Sexual Harassment
- Bullying
- Other violations of AW Group's Code of Conduct

3. How to report

3.1 Staff members and other individuals can file an incident/misconduct disclosure through multiple channels of reporting, available to them by AW Group. The first-hand option shall always be to use ordinary communication channels and to report to manager, management, People and Performance or group legal.

3.2 AW Group has chosen Deloitte as an external service provider to receive and document whistle-blowing reports. This to ensure that all reports are handled by an independent and neutral party without risking conflicts of interests. Deloitte will always ensure that the report is forwarded to an appropriate recipient within AW Group who will be able to investigate the errand independently and with integrity. Deloitte operates 24 hours a day, seven days a week.

3.3 Reports can be made using our Speak Up form, available on all our websites. Through this online platform, individuals can report misconduct provided by Deloitte Halo. Individuals can also ask for the possibility to make the report via telephone instead or request a physical meeting if this is preferred. Requesting a telephone call or a meeting can be done through the Speak Up form.

3.4 Individuals can report misconduct in multiple languages: English, Swedish, Norwegian, Danish, Finnish, German and French.

3.5 The reports are received by Deloitte as an external and independent third-party to AW Group and forwarded to an appropriate recipient within AW Group.

3.6 When reports are made through a telephone call, a physical meeting or in other ways orally, these shall be documented according to what is required by applicable law. The reporting individual will be able to review, correct and approve such documentation.

3.7 When a report is made, Deloitte analysts will review the disclosure and prepare a detailed report, based on the information and evidence provided by the individual who is reporting the incident/misconduct. Upon screening of the report and assessment, the report is forwarded to an AW Group representative, who will investigate the case further within the instances of the AW Group. The representatives are decided by AW Group and will be independent and senior to all parties mentioned within the report. This is further described in Section 6.

4. Anonymity

4.1 All individuals who report an incident/misconduct are free to choose the anonymity level they prefer.

4.2 Individuals can choose to remain totally anonymous, which means that neither AW Group nor Deloitte will be aware of their identity or details.

4.3 Individuals can choose to share their identity or details with Deloitte, as a third-party, which will not share this information with AW Group.

4.4 Individuals can choose to be fully known and provide information on their identity and involvement in the incident that is being reported.

4.5 It is important to provide as much information as possible, to avoid misinformation. However, the whistle-blower will be able to communicate through the Deloitte Halo platform and provide necessary clarifications to their case, without the necessity to share their private information in the disclosure.

5. Feedback

5.1 The whistle-blower will receive confirmation that the report has been received within seven days from making the report, as long as the individual has not asked to not receive a confirmation or if sending a confirmation would reveal the whistle-blower's identity.

5.2 As per the directives from the European Council, AW Group has the obligation to respond and follow up to the whistle-blower's reports within three months. AW Group's representatives will revert with feedback regarding the progress, or the decision taken regarding the misconduct reported.

5.3 The feedback will be available to the individual who reported the issue on the Deloitte Halo platform, or available to be communicated via telephone or physical meeting if this is preferred by the individual.

5.4 The whistle-blower can access the Deloitte Halo platform freely, with no limitations required. Upon submission of their disclosure, they will be provided with username and password, to further access the website and read feedback on their case or, if applicable, add new information and evidence to their previous reported file.

6. Internal management of the report

6.1 Reports made through the Speak Up form in Deloitte Halo, the Speak Up hotline number or a requested meeting through these channels shall always be received and initially documented by Deloitte. This to ensure that all reports are received by an independent and neutral party without risking conflicts of interests. Deloitte is responsible for ensuring that the report is then forwarded to an appropriate recipient within AW Group according to what is stated in this Section 6.

6.2 AW Group's Group General Counsel shall be the primary receiver of whistle-blower reports. A report of an incident/misconduct, either made through Deloitte and the Speak Up service or through regular communication channels, shall immediately be handed over to the Group General Counsel. The Group General Counsel shall handle these reports independently and investigate them without influence of AW Group. The Group General Counsel is responsible for receiving the reports, to conduct the first assessment of the allegations made, and to lead the investigation of the suspected incident/misconduct and the actions taken because of this. The Group General Counsel is also responsible for ensuring that the whistle-blower receives feedback on his/her report within due time and that the errand is properly documented.

6.3 Should a first receiver of the report (either Deloitte or another receiving party within AW Group) find that the Group General Counsels involvement in the errand could trigger a conflict of interests and that the Group General Counsel is therefore not an appropriate receiver of the report internally, the report shall instead be handed over to AW Groups Group People and Performance Director or Group Strategy Director, whichever is more appropriate given the nature of the incident/misconduct. In such a case, they shall have the same responsibilities as stated in Section 6.2.

6.4 During the investigation of the reported incident/misconduct, all persons involved must observe full discretion, in particularly in relation to information that could reveal the whistle-blower's identity. Persons involved in the investigation of the reported incident/misconduct and potential actions taken because of this shall be limited to those who are deemed to be completely necessary to involve. External lawyers or other necessary external resources may be involved only if they are bound by a confidentiality agreement.

6.5 Only those who according to this Section 6 have been considered competent to receive, investigate, act and give feedback on whistle-blower reports shall have access to any personal data processed within the errand. The access shall also be limited to what is completely necessary for the person to conduct his/her tasks related to this. Personal data processed in a whistle-blower errand shall be deleted when they are no longer necessary, but no later than two years after the errand has been closed.

6.6 All reports and other documentation related to a whistle-blower errand shall be deleted when they are no longer necessary, but no later than two years after a potential follow-up errand has been closed.

7. Information about personal data processing

7.1 If you choose to reveal your identity when filing a report, the personal data you provide about yourself will be processed by AW Group and our service provider Deloitte. Your data will only be used for the purpose of investigating the errand you have reported and any communication with you during this process. All personal data you provide about yourself in the report will only be saved for as long as is necessary to fulfill this purpose. The legal ground for processing your data is Academic Works legitimate interest to investigate the errand you have reported and to act against unethical or illegal misconduct. If we disclose your information to law enforcement agencies or regulatory authorities, this will be done with your consent. For more information about our processing of your personal data as well as your rights, please read our Privacy Policy.