Whistleblower policy for all companies in the Aarsleff Group

1. Introduction

The Aarsleff Group has an open corporate culture. Everybody can freely express themselves and report concerns about irregularities or illegal activities concerning the Group's employees, management or suppliers. We find it very important that this type of information comes to light and have chosen to implement a whistleblower scheme.

Per Aarsleff A/S is the data controller for processing personal data necessary for handling of the whistleblower scheme. The Aarsleff Group may be contacted on persondataansvarlig@aarsleff.com or by phoning the Group HR Manager on +45 8744 2222.

The employees are often the first to discover irregularities or unethical behaviour at the workplace. Normally, breaches will be reported to the immediate manager, but often it may be difficult to move forward with information or suspicions due to loyalty issues.

The purpose of the Aarsleff Group's internal whistleblower scheme is to allow the company's employees or anyone else with work-related links to the Aarsleff Group to be able to report in confidence to an impartial unit in the event of reasonable suspicion of violations of EU law within a number of specific areas, serious violations of Danish law or other serious matters, which may inflict financial losses on or in any other way seriously harm the Aarsleff Group and its reputation or the life and health of individual persons.

The whistleblower policy comprises a detailed description of the Aarsleff Group's internal whistleblower scheme, including which offences can be reported, who can do so, how reports will be dealt with and registered, how to use the internal whistleblower scheme, and the rights of the whistleblower and the person concerned.

The purpose of the whistleblower policy is also to inform you about your rights under Act no. 213 of 24 June 2021 on protection of whistleblowers (**"Danish Whistleblower Act"**) as well as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("**General Data Protection Regulation**").

2. Scope

The whistleblower scheme comprises all the companies of the Aarsleff Group.

2.1 Reports covered by the whistleblower scheme?

Reports can be submitted to the whistleblower scheme of (i) breaches of EU law, and which are comprised by the scope of Directive (EU) 2019/1937 of 23 October 2019 on the protection of persons who report breaches of EU law (**"Whistleblower Directive"**) and (ii) other serious breaches of Danish law and EU law and other serious matters.

As regards reports of breaches of the specific EU acts falling within the scope of the Whistleblower Directive, there is no requirement that a serious breach has to be involved. The scope of the Whistleblower Directive covers breaches of EU acts which are thoroughly listed in Part I of the annex to

the Directive, and which, among other things, concern the following areas:

- public procurement
- financial services, products and markets, and prevention of money laundering and terrorist financing
- product safety and compliance
- transport safety
- protection of the environment
- radiation protection and nuclear safety
- food and feed safety, animal health and welfare
- public health
- consumer protection
- protection of privacy and personal data, and security of network and information systems.

Moreover, it comprises breaches detrimental to the EU's financial interests as well as those related to the internal market, including breach of EU competition and state aid rules.

The Whistleblower Directive can be accessed here.

As mentioned above, reports can also be made of serious breaches of Danish and EU law as well as other serious matters. It is possible to report about the following:

1) Serious violations or potential serious violations of existing laws concerning financial crime including but not limited to embezzlement, bribery, corruption, theft, violation of competition laws, fraud and forgery as well as any support to third party regarding such behaviour
2) serious breaches of work safety
3) serious concerns about discrimination, violence and harassment
4) serious breaches of environmental regulations.

Less serious issues as well as employee and employment relationship issues, e.g. dissatisfaction with wages, harassment, incompetence, cooperative difficulties, absence, violation of smoking or alcohol policies or other types of inappropriate behaviour or conduct cannot be reported under the whistleblower scheme. Such issues must be reported through the usual communication channels, e.g. by direct contact with the immediate manager or the HR department. If such issues are reported under the scheme, the report will be deleted, unless it is assessed to be appropriate.

2.2 Who can report to the whistleblower scheme?

All Aarsleff employees, members of the board of directors and other stakeholders may submit a report under the whistleblower scheme.

However, the Aarsleff Group points out that only the following groups of persons are comprised by the special protection of the Whistleblower Act (see more under item 6) and may report breaches they have become aware of in connection with work-related activities: workers, self-employed persons, shareholders, members of the executive management, members of the board of directors, volunteers, paid or unpaid trainees, persons working for contractors, subcontractors and suppliers, persons who report or publicly disclose information acquired in a work-based relationship which has since ended as well as persons whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

Reports can be submitted under the whistleblower scheme even though there is no evidence of the reported information. You must, however, be in good faith as to its accuracy in order to enjoy protection under the Whistleblower Act, see details of the terms of protection under 6.1.

You have the right to submit a report under the whistleblower scheme, regardless of whether you are a Danish citizen or not.

2.3 Persons concerned

Reports can be submitted concerning the persons who have performed acts or have omitted something that is illegal under EU law or who commit a serious breach of the law or some other serious act, or who make it possible to circumvent the purpose of these rules. The person concerned will be the physical or legal person named in the report to the Aarsleff Group's whistleblower scheme as a person to whom the breach can be attributed, or with whom that person is associated.

It is also possible to report activities which cannot be attributed to one individual person but are due e.g. to a basic (system) error in the Aarsleff Group.

3. Reporting procedure

Reports to the whistleblower scheme should be made electronically by completing and sending an online reporting form. The reporting solution is provided by the law firm Kromann Reumert (data processor) and the system provider EQS Group A/S (Got Ethics) (sub data processor). Reports to the whistleblower scheme can be submitted electronically via a link found at www.aarsleff.com under: About Aarsleff / Corporate Social Responsibility.

Reporting can also be made orally to the Group CFO of Per Aarsleff Holding A/S. However, we recommend that reporting takes place by using the online reporting form where reporting can be done anonymously and where the reports are stored in a secure and encrypted IT system.

3.1 Use of incorrect reporting channel

Reporting to the whistleblower scheme cannot take place in any other ways than by using the technical reporting solution or orally to the Group CFO of Per Aarsleff Holding A/S. Consequently, reports cannot be submitted by other means, e.g. by sending an e-mail to the person in charge of the whistleblower scheme, as the report might contain confidential information that should not be transmitted unencrypted. If a report is received by e-mail, the report must be submitted again by using the online reporting form. This may be done by yourself or by the person in the Aarsleff Group who has received the report. If the Aarsleff Group is in contact with you, or your identity is known by the Aarsleff Group, you will be encouraged to submit the report again via the correct channel.

3.2 Confirmation of receipt of a report

If you submit a report electronically, you will automatically receive confirmation of receipt.

3.3 Anonymity

It is up to you whether you want to report anonymously to the whistleblower scheme or if you want to write your contact details, so that Kromann Reumert and/or the Aarsleff Group may contact you with any supplementary or clarifying questions to the report. The Aarsleff Group recommends that you state your name and your contact details in the reporting form. The reason is that experience has shown that

anonymous reports complicate any further investigation as it will not always be possible to ask additional or elaborating questions to the anonymous whistleblower.

It is not possible to report anonymously if you report orally.

In case of anonymous reports, the Aarsleff Group will not attempt to trace the information to a certain person. This also applies even though it may be technically possible, e.g. by tracing the computer's IP address or take other steps to reveal your identity.

Even though you have chosen to be anonymous, the selected IT solution allows Kromann Reumert and/or the Aarsleff Group to contact you via the platform which is used for submission of reports, provided that you have chosen to keep the communication channel open and respond to any additional or supplementary questions which Kromann Reumert and/or the Aarsleff Group may have.

If you want complete anonymity, do not submit a report via:

a) Your work computer or other devices owned by the Aarsleff Group.
b) Your workplace internet connection or similar internet connections administered by your employer.

If you want full anonymity and enclose documents, ensure you have removed metadata from them.

If your report gives rise to investigations made by an external authority, e.g. the police, the Aarsleff Group may be required by law to reveal your identity if the Aarsleff Group is aware of it. If legal proceedings are commenced against the person concerned, you may be called as a witness.

3.4 Rectification and additions

If you become aware that incomplete or misleading information was reported, you should make a new report in which you refer to the previous report and include a description of what should be corrected.

4. How we deal with reports

In the Aarsleff Group, we listen to all whistleblowers, and we take each concern seriously.

The Aarsleff Group has appointed the Group CFO of Per Aarsleff Holding A/S (**"the Whistleblower unit"**) to handle the impartial administration of the Aarsleff Group's internal whistleblower scheme. The whistleblower unit must ensure impartiality and absence of conflicts of interest, and the Group CFO in the whistleblower unit must not receive instruction on how to handle and follow up on specific reports. The whistleblower unit is also bound by a duty of confidentiality.

The technical solution of the whistleblower scheme is supplied and administrated by the law firm Kromann Reumert which – as a data processer employed by the Aarsleff Group – will receive and register received reports.

4.1 Receiving reports

The reports received will be handled by a few trusted employees at Kromann Reumert who will receive the

reports and send them to the Group CFO of Per Aarsleff Holding A/S. If the report concerns the Group CFO, it will be forwarded to the CEO.

4.2 Registration of incoming reports

The Aarsleff Group is obliged to register reports and all documents which the Aarsleff Group or Kromann Reumert has received in relation to reports.

Oral reporting is documented by recording the conversation or meeting, subject to your consent, or by preparing an accurate summary of the meeting or conversation, and you shall be offered the opportunity to check, rectify and accept the document by signing it. Oral reporting made via a telephone line may be documented by making an accurate transcript of the conversation, and you shall be offered the opportunity to check, rectify and accept the document by signing it. For reasons of documentation, oral reporting will be registered in the technical reporting solution. If you wish to be anonymous, your personal data will of course not be registered in the technical reporting solution.

Registration will take place in accordance with the Aarsleff Group's duty of confidentiality, which is further described in item 5.1. This implies that reports are registered in a way which ensures confidentiality of e.g. your identity.

The purpose of the registration is among other things to:

- Ensure evidence is collected from reports received, so that it can be used if required in enforcement proceedings,
- Protect the rights of the person concerned to effective defence in the event of any criminal or other proceedings, for which the information provided could be used as evidence,
- Ensure it is possible to link information from multiple reports on the same matter, when doing so will make relevant response possible, which may not have been possible on the basis of a single report.

Registration of reports shall be made in accordance with the applicable data protection legislation. For an explanation of the criteria used to determine the retention period, see item 8.6 of this Whistleblower policy.

4.3 Obtaining documentation

It is possible for Kromann Reumert to contact you via the platform used for reporting, also if you have submitted anonymous reports to the whistleblower scheme. It is a condition, however, that you have chosen to keep the communication channel open and that you answer potential questions asked via the platform. The documentation may consist of correspondence, documents, photos, minutes from meetings, recordings of telephone conversations, e-mails, expense sheets, internet logs etc. If Kromann Reumert obtains additional documentation from you, and if you choose to be anonymous, all personal information about you will be deleted prior to the disclosure to the relevant persons in the Aarsleff Group.

4.4 Feedback to the whistleblower

The Aarsleff Group will give you feedback on your report as soon as possible and no later than three months from confirmation of receipt.

If in compliance with the law, including relevant rules on the duty of confidentiality, you will be informed of what measures have been taken or are envisaged in response to the report, along with reasons for the

choice of such a response. Such feedback could be that the matter has been passed to the police, an internal investigation has been launched, or a report made to the relevant supervisory authority.

If the Aarsleff Group has not yet determined the appropriate follow-up within three months from confirmation of receipt, you will be informed accordingly, including whether you can expect further feedback.

4.5 Information of persons concerned

In accordance with the General Data Protection Regulation, information must be provided to the persons concerned, and they must be informed about the report within one month. If there is an actual risk that such notification would jeopardise the related investigations, the notification may be postponed for as long as the risk exists.

5. Confidentiality

5.1 Duty of confidentiality

Employees of the Aarsleff Group's Whistleblower unit and employees of Kromann Reumert assisting with the administration of the whistleblower scheme are subject to a duty of confidentiality with regard to the information included in reports to the whistleblower scheme. The duty of confidentiality applies correspondingly to other authorised employees, empowered to receive or follow up on reports, and that may become aware of your identity or other details covered by that duty.

5.2 Disclosure of information about your identity

Information about your identity or other information from which your identity can be disclosed directly or indirectly, cannot be disclosed without your express consent to anyone other than the authorised employees of the Aarsleff Group, empowered to receive or follow up on reports. You may choose to withdraw your consent at any time. However, withdrawal must be without prejudice to the legality of disclosure based on consent prior to withdrawal.

Information about your identity can be disclosed to the public authorities without your consent when required to avoid breaches within the scope of the Whistleblower Act, or with regard to ensuring the rights of the persons concerned to a defence. If the Aarsleff Group intends to disclose information from which your identity can be derived directly or indirectly, the Aarsleff Group must inform you in advance, unless doing so will compromise related investigations or legal proceedings.

Other details taken from reports than those which cannot reveal your identity as the whistleblower can only be disclosed to persons outside the Aarsleff Group's Whistleblower unit and Kromann Reumert when part of the response to a report, or to prevent breaches covered by the scope of the Whistleblower Act. The receiving person will be subject to a duty of confidentiality with regard to the contents, to the same extent as employees of the Aarsleff Group's Whistleblower unit and employees of Kromann Reumert.

6. Protecting whistleblowers

6.1 Conditions of protection

The Whistleblower Act comprises special provisions on protection of whistleblowers against reprisals etc.

Whistleblowers are only covered by the protection of the Whistleblower Act if they have reasonable grounds to believe that the information reported was correct at the time the report was made, and that the information reported comes under the scope of the whistleblower scheme as described above. If you report incorrect information about breaches in good faith, you will also be covered by the protection.

No protection will be given according to the Whistleblower Act if you knowingly report incorrect information, or information on breaches which are groundless, including unsubstantiated rumours and gossip. The consequences of submitting a report in bad faith are described in detail under item 7.1.

You cannot waive the rights you have under the Whistleblower Act.

6.2 Scope of protection

6.2.1 Exemption from liability for breach of the duty of confidentiality and gathering information

If you meet the conditions for protection, you will not be considered to have breached a statutory duty of confidentiality and will not be liable for doing so, provided you had reasonable grounds to believe that the report was necessary to disclose a breach falling within the scope of the Whistleblower Act. Also, you will not be liable for accessing the information reported, provided that such an act does not constitute an independent criminal offence.

6.2.2 Protection against reprisals

If you meet the conditions for protection, you will be covered by the Whistleblower Act's protection against reprisals, including threats and attempts of reprisal as a result of making a report, and you cannot be prevented or an attempt made to prevent you from reporting.

Reprisals are defined as any direct or indirect act or omission occurring in a work-related context as a result of an internal or external report or publication, and which causes or may cause unwarranted harm to the whistleblower.

6.2.3 Application for rejection of legal proceedings

You have the right to invoke a report made to apply for rejection of legal proceedings provided that you had reasonable grounds to believe that the report was necessary to reveal a breach within the scope of the Whistleblower Act.

7. Possible outcomes of reporting

7.1 Consequences for whistleblowers

If you submit a report in good faith, you are protected against any form of adverse consequences.

It may, however, have consequences for you as an employee if incorrect information is knowingly reported, e.g. with the intention of harassing or in some other manner causing harm to other employees or members of the board of directors.

Anyone making a report in bad faith can be subject to disciplinary, civil law (including contract law), criminal law, administrative or employment law sanctions.

7.2 Consequences for persons concerned

Depending on the circumstances, a report may result in the following consequences for the persons concerned:

- disciplinary proceedings against employees concerned which may lead to a warning or termination of employment
- a case brought against board members concerned that can lead to loss of their seat on the board
- the persons concerned can be reported to the police, resulting in criminal charges
- contractual consequences for business partners, e.g. cancellation of a contract.

In principle, a report will not lead to consequences for the persons concerned if the claims in the report are not supported by evidence or by further investigation of the report.

8. Processing of personal data

Collection of personal data provided in connection with a report to the whistleblower scheme and the processing of personal data taking place in connection with a follow up on a report are generally regulated by the data protection legislation, including the General Data Protection Regulation and the supplementary rules of Act no. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (**the Danish Data Protection Act**).

Processing of personal data may take place when it is *necessary* to deal with reports which are received in Aarsleff's whistleblower scheme.

According to the General Data Protection Regulation, data subjects have the right to be informed, this also includes whistleblowers, persons concerned and any third party mentioned in the report. As a result of this obligation to inform, the above sections should be supplemented with the following:

8.1 Categories of personal data

In connection with dealing with a report, Aarsleff will process the personal data stated in the report. The personal data which in particular are processed as part of a report, are identity and contact data as well as a description of the matter/incident which led to the report, including sensitive personal data as well as information about criminal offences and other private matters.

The investigation of the report may also result in collection and processing of further personal data than stated in the report.

8.2 The purposes of and the legal basis for processing of personal data

Aarsleff may process personal data about whistleblowers, persons concerned and other persons which are mentioned in reports when it is necessary to process the reports received in the whistleblower scheme which is established according to the Whistleblower Act.

Processing of personal data may also take place when the processing of such personal data is necessary to follow up on the reports. It may e.g. be the processing of personal data taking place in connection with interviews of relevant job candidates, members of the executive management and board of directors, employment law sanctions as well as information of relevant authorities and filing of a police report.

It is not the intention to collect sensitive personal data, including e.g. data about health, through the whistleblower scheme. However, it may turn out to be relevant and necessary in connection with an investigation of the matters reported (e.g. if matters concerning work safety is to be reported and information about potential work injuries or accidents on the work site must be processed).

The legal basis for the required processing of personal data is described in paragraph 22 of the Whistleblower Act.

8.3 Categories of recipients of personal data

It may be necessary for the Aarsleff Group to disclose personal data from a report to others. As an example, disclosure of personal data to the following categories of recipients may take place:

- Authorised employees of relevant entities/departments within the Aarsleff Group
- Kromann Reumert and any other data processors as well as the EQS Group A/S and any other sub data processors which on behalf of and according to instructions from the Aarsleff Group administer the whistleblower scheme and provide legal, technical and administrative support
- External advisers assisting with e.g. legal assistance in connection with the handling of a specific report
- Public authorities, e.g. the police, if the disclosure takes place in order to address breaches reported.

8.4 Information to be provided to persons concerned and any third party mentioned in reports

Aarsleff must provide information to persons concerned and any third party mentioned in reports about the processing of their personal data in connection with the handling of a report. In principle, specific details must be given to them within a reasonable period after obtaining the personal data, and within one month at the latest. However, the obligation to inform can be postponed or omitted according to specific assessment, e.g. for the sake of investigating a case or if in the overriding interest of Aarsleff, including with regard to the company's business foundation, business practices, knowhow etc. which will outweigh the interests of data subjects. An exemption from the obligation to inform can be made if and when provided for in Article 14 (5) of the GDPR or section 22(1) of the Data Protection Act.

8.5 Transfer to third countries

Personal data, which are collected and stored in the technical whistleblower solution, will not be transferred to a third country, i.e. countries outside of the EU/EEA.

To the extent that the processing of your personal data in connection with the follow-up on a report should imply a transfer to a third country, e.g. by using a hosting supplier established in a country outside the EU/EEA, Aarsleff will, at any time, ensure that such transfer is legal, including that the General Data Protection Regulation's requirements on establishment of an adequate level of protection for the transfer has been complied with, just as you will receive further information.

8.6 Storage of personal data

Reports shall be stored for no longer than it is necessary and proportionate in order to comply with the requirements imposed by the Whistleblower Act. This requires that the period for which the personal data are stored is limited to what is necessary to meet requirements in pursuance of the Whistleblower Act, including particularly the whistleblowers' and the involved persons' potential requirements for obtaining evidence as well as Aarsleff's duty to follow up on reports received, including linking such reports with previously received reports.

It will currently be assessed how long previously received reports should be stored. The specific assessment will include whether it is probable that persons who are entitled to protection according to the Whistleblower Act might have a need to document the report in question. Continued storage may also take place, if there is a legitimate reason, e.g. that the report can be strengthened by reports about the same matter submitted at a later time, e.g. because Aarsleff already has received several reports about the same matter. Continued storage may also be required in order to comply with a legal obligation of other legislation.

If disciplinary sanctions are initiated against a reported employee, or if there are other grounds for which it is relevant and necessary to store the data, the data will be stored in the employee's personnel file. In that case, the personal data must be erased at the latest 5 years after the employee's resignation, unless it is specifically assessed that it is relevant and necessary to store the data, e.g. due to pending legal proceedings.

8.7 Rights of the data subject

As a data subject – i.e. a whistleblower, person concerned or third party mentioned in the report – you have the following specific rights, unless anything else is stated in the data protection legislation:

Right of access
You have the right to have insight into the personal data which we process about you, and to receive a copy of your personal data as well as receive information about:

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipients, including recipients in third countries and in this connection the appropriate safeguards relating to the transfers
- The period for which the personal data will be stored or the criteria used to determine that period
- The right to rectification, erasure, restriction and objection against processing of our personal data
- The right to complain to the Danish Data Protection Agency
- Where your personal data was collected from if they are not collected from you.

Right to rectification
Without undue delay, you have the right to have inaccurate personal data about yourself rectified and the right to have incomplete personal data completed.

Right to erasure ("right to be forgotten")
Without undue delay, you have the right to have personal data about yourself erased where some grounds apply, e.g. if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

Right to restriction of processing
You have the right to obtain restriction of processing of your personal data, e.g. where the accuracy of the personal data is contested.

Right to data portability
You have the right to receive the personal data that you have provided yourself in a structured, commonly used and machine-readable format, and you have the right to have those data transmitted to another controller under certain circumstances.

Right to object
You have the right to object to the processing of your personal data in the context of the processing of a report under the whistleblower scheme. If the objection cannot be refused, the processing of the personal data must stop.

Right to complain to the Danish Data Protection Agency
If you disagree with the way the Aarsleff Group processes your personal data, you have the right to file a complaint to the Danish Data Protection Agency. You can find the contact details of the Danish Data Protection Agency here. However, we hope that initially you will contact us by using the below contact details, so that we can reach an agreement.

You may make use of your rights by contacting persondataansvarlig@aarsleff.com or the Group HR Manager.

9. Breach of the Anti-Money Laundering Act

In the event of a suspicion of a breach of the Anti-Money Laundering Act (Act on Measures to Prevent Money Laundering and Financing of Terrorism), Kromann Reumert may be obliged to report potential breaches to the state prosecutor for serious economic and international crime, and to pass on related details. Such reports will therefore be dealt with in accordance with the rules of the Anti-Money Laundering Act. In such cases, Kromann Reumert will act as an independent data controller and is not in this connection bound by the Aarsleff Group's instructions.

10. The procedure for reporting to external whistleblower schemes

10.1 External whistleblower schemes in brief

An external whistleblower scheme is defined as a whistleblower scheme linked to the public authorities and established under a legal provision requiring that authority to establish an external whistleblower scheme.

Under the Whistleblower Act, an external whistleblower scheme has been established at the Danish Data Protection Agency, where the entire protected group of persons of the Whistleblower Act (and not only employees) can report anything that can also be reported in the Aarsleff Group's internal whistleblower scheme, including reports of breaches of EU law, reports that otherwise relate to serious breaches of the law or other serious matters.

In addition, a number of public authorities have set up external whistleblower schemes for reporting breaches of specific legislation. These include the Danish Financial Services Authority, the Danish Working Environment Authority, the Danish Environmental Protection Agency and the Danish Business Authority.

10.2 The procedure for reporting to external whistleblower schemes

An external whistleblower scheme enables both written and oral reporting, and at your request, reporting can be made via a physical meeting within a reasonable period of time.

If you choose to report to an external whistleblower scheme, you will receive confirmation of the report within seven days of receipt, unless you have expressly requested otherwise or there are reasonable grounds to believe that confirmation of the report would jeopardise the protection of your identity.

The public authority must provide you with feedback on your report within a reasonable period of time, not exceeding three months from the date of receipt, or six months in duly substantiated cases.

You will receive notification of the final outcome of investigations triggered by the report if such notification was not given in connection with feedback.

If the public authority intends to disclose information from which your identity can be derived directly or indirectly, that authority must notify you, unless notification would jeopardise related investigations or legal proceedings.

An external whistleblower scheme can reject reports that are not within the scope of the Whistleblower Act, and is not obliged to forward them to any other authority. In the event of a large influx of reports, an external whistleblower scheme may need to prioritise more serious reports.

10.3 Reporting channel selection

You can choose whether you wish to submit your report to the Aarsleff Group's whistleblower scheme or to a relevant external whistleblower scheme, or both. However, we would like to encourage you to use the Aarsleff Group's internal whistleblower scheme in cases where the breach can be effectively addressed internally and when you do not expect any risk of reprisal.

11. Questions

All questions about the whistleblower scheme should be addressed to Group CFO Mogens Vedel Hestbæk, e-mail: mvh@aarsleff.com or phone no.: +45 8744 2222 or +45 4044 2201.

The Executive Management