WHISTLEBLOWING POLICY

1. Background of this Policy

People who work for or are otherwise in professional contact with a company are often the first to become aware of breaches directed to, involving or taking place in the operations of such company. By reporting breaches of law harming the public interest, such persons act as "*whistleblowers*" and in that way play an important role in detecting and preventing harmful breaches of law. However, potential whistleblowers are often discouraged from reporting their concerns for fear of retaliation.

Largely for these reasons, the European Union has passed legislation, namely the so-called Whistleblowing Directive (EU) 2019/1937 ("**Directive**"), to set EU-wide minimum standards for the effective protection of whistleblowers reporting breaches of particularly important EU-level legislation. In turn, the EU member states have implemented these minimum standards in their national laws. In Finland the implementation has been carried out by passing so-called Whistleblowing Act. (Directive and Act are jointly referred to as the "**Legislation**").

2. General

We at Mitta Group Oy, Mitta Oy and other legal entities in the same group of companies having their principal place of business in Finland (hereinafter collectively referred to as the "**Company**") are in addition to compliance of applicable laws committed to a high level of ethics and integrity when conducting our business operations. We understand that this is crucial to our success and reputation. Our values, principles and policies guide our everyday business operations. We have a responsibility to speak up and report corrupt, illegal or other undesirable conduct and take appropriate action after such conduct is detected. This Whistleblowing Policy (hereinafter "**Policy**") is an important legal tool for detecting such conduct. The Company strongly encourages you to report if you suspect or witness such conduct, activity or behavior. Company assures you that all reports made under this Policy will be taken seriously.

If you submit a whistleblowing report in accordance with this Policy, the Company have a responsibility to protect you, including concealing your identity and ensuring you are not subject to any retaliations.

This Policy specifies how the Company will provide you with an effective, objective, confidential and secure electronic whistleblowing reporting channel (hereinafter the "**Whistleblowing Channel**") allowing you to express your concerns or suspicions openly and safely. On the Whistleblowing Channel, you are also advised how to make a report, how you are informed on the follow-up actions and how you are protected. The Company will review the Policy and the Whistleblowing Channel from time to time to ensure that it is accurate and proper and functioning reliably.

The Whistleblowing Channel is not intended for reporting personal work-related grievances, such as grievances related to an employment contract or occupational health and safety. These are subject to the Company's other policies and reporting procedures. Accordingly, the Whistleblowing Channel should not be used to provide general feedback to the Company.

This Policy and the Whistleblowing Channel have been prepared in accordance with Legislation and the Company complies with such Legislation.

3. Information to be Reported

Actual and potential breaches and arrangements which can be reported in the Whistleblowing Channel are closer specified in the Section 2 of the Act with the exceptions specified in the Section 4 of the same Act. Given the Company's business area and activities, to the Company's understanding, the most material areas and issues to be reported relate to privacy and personal data, security of network and information systems as well as competition rules. All breaches and arrangements reportable under applicable legislation are hereinafter referred to as "**Breaches**".

When you have information or reasonable suspicion of an actual or potential Breach that has occurred or is likely to occur in the Company, or an attempt to conceal such Breach, please report it through the Whistleblowing Channel.

If you are uncertain, you can first submit a question through the Whistleblowing Channel to ask whether the information you intend to disclose is in the scope of the Legislation and can be disclosed through the Whistleblowing Channel. Please remember to include at least your email address in connection with the submission so that the person handling your request can effectively respond to you through the Whistleblowing Channel.

The Whistleblowing Channel is available 24/7. The questions presented in the Whistleblowing Channel will guide you to provide the information necessary to investigate and handle your report. Kindly answer all questions as accurately as possible.

4. Eligible Whistleblower

Persons eligible to act as whistleblowers and submit a report concerning the Company are the persons who are in employment or director relationship with the Company and have acquired information on Breaches within their work or in work-related context] OR [all persons who have acquired information on Breaches within work or in work-related context while being in a following position: Company's employee, director, self-employed person, agency worker, volunteer worker, trainee, shareholder who plays an active role in the Company, member of Board of Directors or Administrative Board, or Managing Director of the Company.

Your right to report Breaches is unlimited and cannot be limited or waived by, e.g. any agreement, policy, form or terms of employment.

5. Anonymity

You can submit a report on a suspected Breach and its potential perpetrator anonymously through the Whistleblowing Channel. All reports coming through the Whistleblowing Channel are confidential meaning that the Company has the obligation to protect and keep your identity and the identity of any third party possibly mentioned in your report confidential. The reporting service is entirely independent of the Company to ensure that it is impossible to find out who is behind a report, for example by tracking IP addresses.

5.1. Levels of Anonymity

When submitting a report to the Whistleblowing Channel, you must first choose whether you want to do so anonymously or whether you want to disclose your identity fully to the persons designated to receive and handle your report ("**Handlers**").

5.1.1 Submitting report anonymously

When you submit a report in the Whistleblowing Channel, you will always receive a unique report-specific link to see the status of your report and to see any follow-up questions the Handlers may have had. You cannot be identified through this link. The link is provided only for the purpose to contact you anonymously when needed. If you have chosen to submit a report to the Whistleblowing Channel anonymously, you must choose between the following two levels of anonymity:

1. Providing e-mail address to receive notifications of new questions or information

   When submitting your report, you can choose to provide your email address to the Whistleblowing Channel through which you will receive an email notification if a question or a notification has been sent to you concerning your report. Your email address is only used by the technical platform of the Whistleblowing Channel and will serve as a technical tool to notify you of new events. The Company and the Handlers do not see or receive information about your email address. All information related to a report is erased from the Whistleblowing Channel when the

report has been processed so that no sensitive information is stored unnecessarily. This primarily takes a maximum of three (3) months.

2. Full anonymity

You may also leave a report in the Whistleblowing Channel without disclosing your name, identity or providing your email address at all. In this case, the Handlers will still be able to contact you through the link you received after submitting the report, but you yourself are responsible for remembering the link and reviewing it from time to time to see if there are any updates or follow-up questions to your report. You will not be notified of these through your email. If you choose not to disclose your name/identity and provide your email address to the Handlers, this may prevent the handling of your report and performing follow-up actions as effectively as the Company would like to. Correspondingly, this may prevent ensuring that there exists no conflict of interest between you and the Company's designated representatives chosen to further investigate the report (also Handlers).

5.1.2 Submitting report by fully disclosing your identity

When you provide your name or other information disclosing your identity in addition to your email address in the Whistleblowing Channel, only the Handlers will receive this information. The Handlers are obliged to keep your name, identity and any other information from which your identity can be discovered confidential unless they are authorized under the Legislation to disclose the information (e.g. if the information needs to be provided on to the police or other authorities) or if you give your explicit consent to reveal such information. In this case information on your name and identity as well as any other information from which your identity can be discovered including your email address are also deleted from the technical platform of the Whistleblowing Channel permanently after the handling of your report in the Whistleblowing Channel is concluded.

As a whistleblower you have the right to be informed in advance if your identity will be disclosed, unless such disclosure would obstruct the purpose of assessing the accuracy of the report, preliminary judicial investigation or litigation.

6. Offered Protection

You will receive protection against retaliation, i.e. negative consequences, threats and attempts of retaliation that may result from your report:

- if you are eligible whistleblower as specified in Section 4 of this Policy; and
- if you have reasonable grounds to believe that the information you report is true and falls within the scope of the Legislation at the time of reporting; and
- if you have reported the Breach in accordance with the so called three-step system. In order to comply with the three-step system you must primarily use our Whistleblowing Channel to report the Breach.

In addition, if you are employed by the Company at the time of reporting, please note that in order to comply with your statutory duty of loyalty towards the Company as your employer, you must primarily use our Whistleblowing Channel to report Breaches (first step in the three-step system).

However, you do not need to use our Whistleblowing Channel to get protection if:

- you are not allowed to access our Whistleblowing Channel; or
- you have reasonable grounds to believe that the Company has not taken actions required primarily within three (3) months period of time from the receipt of your report e.g. the Company has not provided you any follow-up on the actions performed primarily within three (3) months period of time from the receipt of your report; or

- you have reasonable grounds to believe that the Company is not able to intervene efficiently with the Breach e.g. when using our Whistleblowing Channel could endanger the investigation of the Breach or the Breach requires urgent action to protect, for example, human life, health or safety or the environment; or
- you have reasonable grounds to believe that you run the risk of retaliation due to your report e.g. you have breached your contract based confidentiality obligation by reporting the Breach or the object of your report has started to threaten you with retaliation already when you are preparing your report.

In such situations, you are also entitled to report the Breach through the public channel provided by the authority (Office of the *Chancellor of Justice is responsible for maintaining centralized channel*) and still receive protection (second step of the three-step system). When using the public channel, you cannot submit a report anonymously. Please note that the reference to public refers here to a specific public whistleblowing channel maintained by the *Office of the Chancellor of Justice or other regulated authority*, not to public disclosure of information to the general public, such as online or to newspapers (this is only the third possible step of the three-step system and thus primarily the last alternative). The public disclosure of information to the general public is justified only in rare situations. Such situation may be at hand e.g. if you have reasonable grounds to believe that Breach can with a high probability cause immediate danger to general interests such as to people's life or health (such as a Breach related to nuclear and radiation safety). For avoidance of doubt, contacting your trade union regarding issues related to your employment or requesting legal assistance from your trade union lawyer or other instant in relation to reporting procedure is not deemed as general disclosure of information to the general public.

Please note that you are not obliged to first report through our Whistleblowing Channel or through the public channel provided by an authority in order to receive protection if you report Breach directly to EU institution or body.

In short, the protection provided to you includes:

- identity protection; and
- protection from retaliation and possible reversal of the burden of proof in the handling of claim related to retaliation in the courts and other authorities; and
- possible compensation and remedies e.g. due to retaliation; and
- possible protection against civil, criminal and administrative liability.

Please note that you do not have to prove that the information you have reported is correct. If you have been eligible whistleblower as specified in Section 4 of this Policy, you have had reasonable grounds to believe that the facts you have reported are true at the time of reporting and fall within the scope of the Breaches and you have complied with the three-step system, you are entitled to protection even if your report later turns out to be incorrect. Please note that a mere allegation or hearsay without supporting information is unlikely to meet the required reasonable grounds standard. Please also note that no protection is available if you report on information that has already been published.

Knowingly submitting a false report is a breach of the Legislation and our Code of Conduct and may result in disciplinary action. Knowingly submitting a false report may also lead to other legal consequences such as obligation to pay damages.

In addition to the protection provided to the whistleblower, the Company also provides protection to the persons suspected of having committed the Breach. This protection includes, e.g. that the suspected persons will be treated equally and in a non-discriminatory manner and that the consequences of the Breach are based on the Company's policies and applicable laws. Such persons are

also granted the opportunity to review and comment on the alleged Breach and related materials to the extent required by the Legislation. Further, such persons may be entitled to compensation due to deliberate false report.

7. Receipt and Preliminary Review of Report

Our Whistleblowing Channel is designed, established and operated in a secure manner that ensures the confidentiality of your identity and the identity of any third parties mentioned in your report. Access to your report is prevented from persons who are not the Handlers. In addition, the Handlers are subject to statutory non-disclosure obligation specified in the Legislation.

In order to create a credible Whistleblowing Channel for reporting Breaches, to ensure objectivity in the handling of reports and to avoid reports being handled by a person who is in any way connected to the reported Breach, the Company has decided to use the following third-party service providers to provide and maintain the Whistleblowing Channel:

a) Lantero AB, a reputable provider of whistleblowing systems; and
b) HH Partners Attorneys-at-law Ltd. acting as the preliminary handler of the whistleblowing reports;

(hereinafter collectively referred to as "**Service Provider**").

Due to the third-party Service Provider arrangement, the persons who are designated to receive and perform the preliminary review of your whistleblowing report are impartial, independent and professional.

All whistleblowers will receive confirmation of receipt of their reports as soon as their reports have been received and at the latest within seven (7) days of the submission of their reports. Please note that only those who have provided their email address at the time of reporting will be notified by email of the confirmation of the receipt of their report. Others are responsible for checking the status of their report via the link provided after the submission of their report.

The Handlers may also request further information from whistleblowers through the Whistleblowing Channel. You as the whistleblower are not obliged to provide further information, however, this would be highly appreciated. Please note that only those who have provided their email address at the time of reporting will be notified by email of any additional questions related to their report. Others should independently check from time to time for any additional questions relating to their reports via the link provided after the submission of their report.

Whistleblowers will receive feedback concerning their reports primarily within three (3) months from the confirmation of receipt. Feedback means information on the follow-up actions envisaged or taken by the Company and the grounds for the choice of those follow-up actions. Please note that adequate feedback can also be information on ending the handling of the report if e.g. no sufficient clarification is available or the Breach is minor and has already ended. Please note that the Company may be unable to disclose details in its feedback, especially due to possibly applicable mandatory legal requirements. Again, please note that only those who have provided their email address at the time of reporting will be notified by email of possible feedback. Others are responsible for checking the status of their report via the link provided after the submission of their report.

All received reports are recorded in the case management register or registered otherwise.

The Company has unilateral right to decide on the change of the Service Provider to another service provider by informing on such change.

8. Internal Handling of Report

After the Service Provider has received and preliminarily reviewed your report, the Service Provider may report the case to at least two Handlers of the Company. Such report made by the Service

Provider shall be prepared by maintaining confidentiality. The designated Handlers of the Company are the following:

- Chairman of the Board of Directorsof Mitta Group Oy, Timo Hyvönen, and
- Members of the Board of Directors of Mitta Group Oy and
- Managing Director of Mitta Group Oy, Henrik Malmberg; and
- Chief Financial Officer of Mitta Group Oy, Anne Antson; and
- Compliance Manager of Helmet Capital, Sanna Hautala.

Since this Policy and the Whistleblowing Channel cover all legal entities in the Mitta Group Oy group of companies in Finland, the Service Provider shall take into consideration, which legal entity is at each time subject to the report, when deciding the correct Handlers of the said legal entity to whom information related to the report will be reported.

The Service Provider will decide whether your whistleblowing report requires further investigation and to whom of the Handlers of the Company the report will be delivered with the objective to ensure that there cannot exist any conflict of interest between the Handlers of the Company, you and the persons named in your whistleblowing report or associated with the Breach mentioned in your whistleblowing report.

The Handlers of the Company will decide on any further investigation and action required to be taken by the Company. All such investigations and any follow-up actions shall be conducted in a diligent manner maintaining confidentiality. The Company will report any possible criminal offences to the police. In other cases, possible actions are e.g. providing guidance to the personnel on the correct procedure and changing procedures that resulted in the Breach.

The Company reviews the performance, expertise, experience and impartiality of the Handlers on a regular basis and has unilateral right to change these Handlers, if necessary, merely by informing on such changes.

The Company has unilateral right to decide on qualification requirements as well as scope of the tasks and powers of the Handlers. The Company also has unilateral right to decide on changes to these merely by informing on the changes.

9. Data Protection

The Whistleblowing Channel is subject to data protection legislation. The Company has conducted a data protection impact assessment as required by the applicable Legislation.

10. Raising concerns about Actions taken by Company

If you are concerned that:

- you may be, are being, or have been subjected to retaliation; or
- there has been a disclosure of your identity or any third parties mentioned in your report contrary to this Policy; or
- your report has not been handled in compliance with this Policy and/or Legislation;

we kindly ask you to proceed as follows:

Please send a new report via the Whistleblowing Channel with a clear reference to "*Concerns about actions taken*". Upon receipt of such a report, the Service Provider will decide to whom information on your report should be delivered with the objective that there cannot exist any conflict of interest between the Company's Handlers and you. The Company's Handlers are defined above in Section 8 (“Internal Handling of Report”) of this Policy. As stated in Section 6 (“Offered Protection”) of this

Policy, you also have the right, in certain circumstances, to report using the specific public whistleblowing channel provided by authorities or even publish your information.

Please note that if you choose to keep your identity confidential in a situation where you are concerned that you may be, are or have been subject to retaliation, the Company may not be able to investigate and respond to suspected retaliation against you as effectively as the Company would like.

11. Informing and Training

The Company will provide information and training related to the Whistleblowing Channel as and to the extent deemed necessary by the Company. The Company has a unilateral right to choose the way of organizing the informing and training. The Company may for instance choose to organize informing and training by internal training, by a website or by using outside service provider.

12. Security of the Whistleblowing Channel

The Company and its Service Provider are committed to monitor the information security of the Whistleblowing Channel on a regular basis in accordance with the Legislation.

13. Amendments

The Company reserves the right to amend and change this Policy unilaterally at any time excluding such matters for which cooperation negotiations are required under the applicable mandatory laws.