MITTA

# WHISTLEBLOWING POLICY

## 1. General

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

If you submit a whistleblowing report in accordance with this Policy, we 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 prepared have been prepared and the Company complies with the requirements of the whistleblowing directive (EU) 2019/1937 ("**Directive**") and local Swedish act "*Lag (2021:890) om skydd för personer som rapporterar om missförhållanden*"("**Act**") (Directive and Act are jointly referred to as the "**Legislation**").

## 2. Concerns and Suspicions to be Reported

Actual and potential breaches and arrangements which can be reported in the Whistleblowing Channel are those specified in Chapter 1, Section 2 of the Act, with the exceptions specified in Chapter 1, Section 3 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 grounds to assume an actual or potential Breach 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 regulation 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.

## 3. Eligible Whistleblower

Persons eligible to act as whistleblowers and submit a report concerning the Company are all persons who, by virtue of their work or in connection with their whether or not paid, have access to information on Breaches while being in a position, including, but not limited to, the Company's employees, directors, self-employed persons, agency workers, volunteers and trainees, shareholders who play an active role in the Company and members of Board of Directors or Administrative Board and 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.

## 4. Anonymity

You can submit a report on a suspected Breach and its potential perpetrator anonymously through our 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.

### 4.1. 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 authorized and appointed to receive and handle your report ("**Handlers**").

#### *4.1.1 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. It is 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 representatives chosen to further investigate the report.

#### *4.1.2 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 Act to reveal the information (e.g. if the information needs to be passed 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.

You have the right, where applicable, to be informed if information that can identify you as the reporting person will be disclosed, unless such information would prevent or obstruct the purpose of the planned measures.

## 5. Offered Protection

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

- the reported matter has occurred, or is highly likely to occur, in the business in which you are active in, have been active in or may become active in, or if the reported matter has occurred, or is highly likely to occur, in another business that you are in contact with, or have been in contact with, through your work,
- you have reasonable grounds to believe that the matter you report is true and fall within the scope of the Act at the time of reporting; and
- you have reported internally, externally or through a publication in accordance with Chapter 4, Sections 4-9 of the Act.

### 5.1. Internal reporting

The protection also applies if you report internally in a way other than via the Whistleblowing Channel if the channel and its procedures of some reason do not meet the requirements of the Act, or if you file a report before you have started your work within the Company.

### 5.2. External reporting

You will also receive protection against retaliation if you submit a report to one of the designated external public whistleblowing channels provided by authorities, which are specified in the Swedish regulation "*Förordning (2021:949) om skydd för personer som rapporterar om missförhållanden*" ("**Regulation**").

A table of the current external reporting channels according to the Regulation are included in Appendix A.

The protection also applies if you report externally to an authority in another way than via an external reporting channel, provided that you

- first reported internally in accordance with the Act, but we have not taken reasonable actions due to the reporting, or we have not, to a reasonable extent, provided feedback on the report

MITTA

within three (3) months from the receipt of your report, or, if you have not received any confirmation on your report and the reason for the non-response is not due to you; seven (7) days from the receipt of the report;

- have reasonable grounds to believe that the Breach requires urgent action to protect, for example, human life, health or safety or the environment; or
- has reasonable grounds to assume that an internal report would involve a risk of reprisals or lead to the Breach not being likely to be remedied in an effective manner.

The protection also applies when reporting a Breach to any of the EU institutions, bodies and agencies that have established external reporting channels and procedures to receive reports of Breaches, provided that you report in accordance with the procedures that apply to the relevant reporting channel.

### 5.3. External publication

The protection finally applies if you publish the information externally, provided that you

- first reported internally in accordance with the Act, but we have not taken reasonable actions due to the reporting, or we have not, to a reasonable extent, provided feedback on the report within three (3) months, or, if there are special reasons; six (6) months and you have been informed about the reasons for extending the deadline, from the receipt of your report,
- have reasonable grounds to believe that the Breach requires urgent action to protect, for example, human life, health or safety or the environment; or
- has reasonable grounds to assume that an internal report would involve a risk of reprisals or lead to the Breach not being likely to be remedied in an effective manner.

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 for reporting procedure is not deemed as general disclosure of information to the general public.

### 5.4. Summary

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 your suspicions or allegations are correct. If you have had reasonable grounds to believe that the facts you have reported are true and fall within the scope of the Breaches and you have complied with the Act, 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.

Knowingly submitting a false report is a breach of the Act our Code of Conduct and may result in disciplinary action. Knowingly submitting a false report may also lead to other legal consequences.

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 Act.

## 6. 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 Act.

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 whistleblower systems; and
b) HH Partners Attorneys-at-law Ltd. acting as the preliminary Handler of the whistleblowing reports
c) Glimstedt AB lawfirm which operate as consults in matters regarding Swedish legislation

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

Due to the third-party Service Provider arrangement, the persons who are authorized and appointed 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.

According to the Act, whistleblowers also have a legal right to report orally and, if requested, at a physical meeting within a reasonable time.

**If you prefer submitting your report orally or in a physical meeting instead of using the Whistleblowing Channel, please see contact details for such a procedure below:**

+46706-201108
annie.ekstrom@mitta.se
HR&Salaries
Mitta AB

## 7. Internal Handling of Report

After the preliminary Handlers of the Service Provider has received and preliminarily reviewed the report you have provided, the Service Provider may report the case to at least one Handler of the Company. Such report made by the Service Provider shall be prepared by maintaining confidentiality. The Handlers of the Company are the following:

- Chairman of the Board of Directors of Mitta Group Oy, Timo Hyvönen, and
- Members of the Board of Directors of Mitta Group Oy; and
- Managing Director of Mitta Group Oy, Aki Puska, and
- Compliance Manager of Helmet Capital, Sanna Hautala.

Since this Policy and the Whistleblowing Channel cover all legal entities in the Mitta group of companies in Sweden, if the reported case involves a specific subsidiary or parent company, the Service Provider will consider this when choosing the correct person and report the case to authorized and appointed Handler of the legal entity in question.

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

The authorized and appointed Handlers in 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.

## 8. Freedom of communication and acquisition

Under Swedish law, you are covered by the Freedom of the Press Act "*Tryckfrihetsförordningen*" ("**TF**") and the Freedom of Expression Act "*Yttrandefrihetsgrundlagen*" ("**YGL**"). TF and YGL are Swedish regulations on freedom of information and freedom of acquisition. Freedom of information is the right, but not the obligation, of every citizen to provide information on any subject for publication and publication in constitutionally protected media. This right also applies to a certain extent to classified information such as information from non-public documents. Freedom of acquisition can be seen as an extension of the freedom of information and gives the right to acquire the information for the purpose of publishing or publishing it.

Please note that the freedom of communication and the freedom of acquisition do not mean that a private employer, such as the Company, is prevented from investigating the source of the information and take measures against such actions. Communication of information can thus, for example, be a breach of both confidentiality and loyalty which is something the Company may take action against.

## 9. Data Protection

The Whistleblowing Channel is subject to data protection legislation.

The collected personal data depends on the information you have chosen to provide in connection with your report. The collected personal data can be divided into contact details, content data, system data as well as any optional and additional information necessary for the investigation of the report. Contact details include e.g. your name and email address provided that you have opted to provide such in connection with filing of your report. Content data includes the content and timing of your report, excluding your name and email address. System data includes technical log information on the use of the Whistleblowing Channel, excluding your name and email address. Any optional and additional information necessary for the investigation of the report (relating to an identified or identifiable natural person) include information you have recorded about yourself or others.

The personal data is processed for the purpose of reporting and investigating reports of alleged violations of applicable laws in relation to our activities as well as to enable review of the reports and disclosure of the results of the investigation to the parties involved. The legal bases for processing are our legal obligations and our legitimate interests.

We retain your personal data only as long as and to the extent which we have a legitimate reason to retain it for the purposes described above. To determine the appropriate retention period, we consider and evaluate the scope, nature and sensitivity of the personal data we process, the potential risk of harm or damage from unauthorized use or disclosure, the purposes for which we process the data and the relevant legal requirements. Having said the above, we will delete the personal data coming through the Whistleblowing Channel within two (2) years of receiving the report unless their retention is necessary for the implementation of the rights or obligations under law or for the establishment, exercise or defence of legal claims. We will also regularly assess the data we keep, and where we deem retention unnecessary, we will delete the data without undue delay.

For further information regarding our processing of personal data and your rights as a data subject, please see our Privacy Policy here. 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;

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 the report should be delivered with the objective that there cannot exist any conflict of interest between the Company's Handler and you. The Company's Handlers are defined above in Section 7 of this Policy. As stated in Section 5 of this Policy, you also have the right 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.

MITTA

## Appendix A – Table of external reporting channels (as per January 2023)

On this page you will find a list of all authorities and their responsibilities in the event of whistleblowing.

| *Myndighet* | *Ansvarsområde enligt förordning 2021:949* |
|---|---|
| **Arbetsmiljöverket** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden som inte omfattas av någon annan behörig myndighets ansvarsområde. |
| **Boverket** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| **Elsäkerhetsverket** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| **Ekobrottsmyndigheten** | Missförhållanden inom området EU:s finansiella intressen enligt artikel 2.1 b i Europaparlamentets och rådets direktiv (EU) 2019/1937, när det gäller bedrägeribekämpning. |
| **Fastighetsmäklarinspektionen** | Missförhållanden inom området finansiella tjänster, produkter och marknader och förhindrande av penningtvätt och finansiering av terrorism och som omfattas av myndighetens tillsynsansvar. |
| **Finansinspektionen** | Missförhållanden inom området finansiella tjänster, produkter och marknader och förhindrande av penningtvätt och finansiering av terrorism och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området konsumentskydd och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området skydd av privatlivet och personuppgifter samt säkerhet i nätverks- och informationssystem och som omfattas av myndighetens tillsynsansvar. |
| **Folkhälsomyndigheten** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området folkhälsa och som omfattas av myndighetens tillsynsansvar. |

| | |
|---|---|
| **Havs- och vattenmyndigheten** | Missförhållanden inom området miljöskydd och som omfattas av myndighetens tillsynsansvar. |
| **Integritetsskyddsmyndigheten** | Missförhållanden inom området skydd av privatlivet och personuppgifter samt säkerhet i nätverks- och informationssystem och som omfattas av myndighetens tillsynsansvar. |
| **Inspektionen för strategiska produkter** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| **Inspektionen för vård och omsorg** | Missförhållanden inom området folkhälsa och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området skydd av privatlivet och personuppgifter samt säkerhet i nätverks- och informationssystem och som omfattas av myndighetens tillsynsansvar. |
| **Kemikalieinspektionen** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området miljöskydd och som omfattas av myndighetens tillsynsansvar. |
| **Konsumentverket** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området folkhälsa och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området konsumentskydd och som omfattas av myndighetens tillsynsansvar. |
| **Konkurrensverket** | Missförhållanden inom området offentlig upphandling och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området den inre marknaden enligt artikel 2.1 c i Europaparlamentets och rådets direktiv (EU) 2019/1937, när det gäller konkurrensområdet. |
| **Livsmedelsverket** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området miljöskydd och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området strålskydd och kärnsäkerhet och som omfattas av myndighetens tillsynsansvar. |

| | |
|---|---|
| | Missförhållanden inom området livsmedels- och foder-säkerhet, djurs hälsa och välbefinnande och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området skydd av privatlivet och personuppgifter samt säkerhet i nätverks- och informationssystem och som omfattas av myndighetens tillsynsansvar. |
| **Läkemedelsverket** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området folkhälsa och som omfattas av myndighetens tillsynsansvar. |
| **Länsstyrelsen Blekinge, Länsstyrelsen i Dalarnas län, Länsstyrelsen Gotlands län, Länsstyrelsen Gävleborg, Länsstyrelsen i Hallands län, Länsstyrelsen i Jämtlands län, Länsstyrelsen i Jönköpings län, Länsstyrelsen Kalmar län, Länsstyrelsen i Kronobergs län, Länsstyrelsen i Norrbottens län, Länsstyrelsen Skåne, Länsstyrelsen Stockholm, Länsstyrelsen i Södermanlands län, Länsstyrelsen i Uppsala län, Länsstyrelsen Värmland, Länsstyrelsen Västerbottens, Länsstyrelsen i Västernorrlands län, Länsstyrelsen Västmanlands län, Länsstyrelsen i Västra Götaland, Länsstyrelsen i Örebro län, Länsstyrelsen Östergötland,** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens ansvar för tillsynsvägledning. |
| | Missförhållanden inom området miljöskydd och som omfattas av myndighetens ansvar för tillsynsvägledning. |
| **Länsstyrelserna i Stockholms, Västra Götalands och Skåne län har dessutom följande ansvarsområde** | Missförhållanden inom området finansiella tjänster, produkter och marknader och förhindrande av penningtvätt och finansiering av terrorism och som omfattas av myndighetens tillsynsansvar. |
| **Myndigheten för samhällsskydd och beredskap** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar |
| **Naturvårdsverket** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området miljöskydd och som omfattas av myndighetens tillsynsansvar. |

| | |
|---|---|
| **Post- och telestyrelsen** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området skydd av privatlivet och personuppgifter samt säkerhet i nätverks- och informationssystem och som omfattas av myndighetens tillsynsansvar. |
| **Regeringskansliet** | Missförhållanden inom området EU:s finansiella intressen enligt artikel 2.1 b i Europaparlamentets och rådets direktiv (EU) 2019/1937, när det gäller statsstödsområdet. |
| | Missförhållanden inom området den inre marknaden enligt artikel 2.1 c i Europaparlamentets och rådets direktiv (EU) 2019/1937, när det gäller statsstödsområdet. |
| **Revisorsinspektionen** | Missförhållanden inom området finansiella tjänster, produkter och marknader och förhindrande av penningtvätt och finansiering av terrorism och som omfattas av myndighetens tillsynsansvar. |
| **Skatteverket** | Missförhållanden inom området EU:s finansiella intressen enligt artikel 2.1 b i Europaparlamentets och rådets direktiv (EU) 2019/1937, när det gäller skatteområdet. |
| | Missförhållanden inom området den inre marknaden enligt artikel 2.1 c i Europaparlamentets och rådets direktiv (EU) 2019/1937, när det gäller bolagsskatteområdet. |
| **Skogsstyrelsen** | Missförhållanden inom området miljöskydd och som omfattas av myndighetens tillsynsansvar. |
| **Spelinspektionen** | Missförhållanden inom området finansiella tjänster, produkter och marknader och förhindrande av penningtvätt och finansiering av terrorism och som omfattas av myndighetens tillsynsansvar. |
| **Statens energimyndighet** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området skydd av privatlivet och personuppgifter samt säkerhet i nätverks- och informationssystem och som omfattas av myndighetens tillsynsansvar. |
| **Statens jordbruksverk** | Missförhållanden inom området miljöskydd och som omfattas av myndighetens tillsynsansvar. |

| | |
|---|---|
| | Missförhållanden inom området livsmedels- och foder-säkerhet, djurs hälsa och välbefinnande och som omfattas av myndighetens tillsynsansvar. |
| **Styrelsen för ackreditering och teknisk kontroll** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| **Strålsäkerhetsmyndigheten** | Missförhållanden inom området strålskydd och kärnsäkerhet och som omfattas av myndighetens tillsynsansvar. |
| **Transportstyrelsen** | Missförhållanden inom området produktsäkerhet och produktöverensstämmelse och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området transportsäkerhet och som omfattas av myndighetens tillsynsansvar. |
| | Missförhållanden inom området skydd av privatlivet och personuppgifter samt säkerhet i nätverks- och informationssystem och som omfattas av myndighetens tillsynsansvar. |