Whistleblowing policy for Amplex, KAMIC Group and Mindelon

Background

In our corporate groups Amplex, KAMIC Group and Mindelon, we endeavour to have an open and transparent workplace, where misconduct and serious negligence should not occur. Our basic approach is that leadership and teamwork should be characterised by respect, clarity and a healthy balance between responsibility and authority. Employees in our Sphere are encouraged to turn to their immediate manager, the business area manager or the HR function in the event of any misconduct. Such reporting should, as far as possible, be treated and handled confidentially and should never lead to any negative consequences for the informant.

However, there may be situations where an employee does not feel comfortable to report openly and directly to someone, for example when the matter concerns a senior manager. It is therefore important to us that it is also possible to report anonymously. It is crucial that the business area management and/or group management receive information about misconduct and problems so that we can take corrective action as soon as possible. In this way, we work together to promote the trust of our employees, customers and the general public.

Amplex, KAMIC Group and Mindelon comply with current whistleblowing legislation. This whistleblower policy therefore covers the legal entities Siga Electronics Ltd, AGW Electronics Ltd, Avon Magnetics Ltd, Advanced Handling Ltd, Astley Signs Ltd, NT Magnetics s.r.o., Movomech AB, Eltecno i Vellinge AB, Kamic Installation AB, and Finelcomp Oy. Other companies within our groups may also adopt and use this policy.

For definitions of terms used in this policy, see section 7.

1. Who can blow the whistle?

You can blow the whistle and receive protection under the Whistleblowing Act if you are an employee, job applicant, trainee or consultant in one of our companies, or an active shareholder or board member. The fact that you have ended your work-related relationship with us, or that it has not yet started, does not prevent you from reporting misconduct.

2. What can I blow the whistle on?

If you suspect misconduct, we encourage you to report this to us as a whistleblowing case. You do not need to have concrete evidence to support your suspicion, but you should have reasonable grounds to believe that the information you provide is true and that reporting the information is necessary to uncover the reported misconduct. The whistleblowing facility must be used responsibly and abuse of the system will not be tolerated.

2.1 Misconduct of public interest

You can report information about serious misconducts and irregularities that have emerged in a work-related context and where there is a public interest in correcting or terminating the misconduct. However, personal complaints and dissatisfaction that are not in the public interest, such as questions about your own work situation or your employment conditions, are not covered. For such issues, we encourage you to contact your immediate manager, the HR function or other appropriate responsible person. This is to ensure that these matters are handled in the best possible way.

Examples of misconduct of a serious nature that you should report:

- Financial crime such as deliberate false accounting, embezzlement, bribery, corruption, money laundering, breach of sanctions rules and terrorist financing.
- Theft, vandalism, fraud or data breaches.
- Serious environmental offences or major breaches of safety in the workplace.
- Serious forms of discrimination or harassment.
- Other serious misconduct that could have negative consequences for the vital interests of our companies.

The above list is not exhaustive but should be considered as examples of events to be considered as misconduct.

2.2 Misconduct contrary to EU law

There is also the possibility to report information about misconduct in a work-related context that is contrary to EU legal acts or provisions. Examples include misconduct relating to public procurement, environmental protection, food safety, public health and the protection of personal data. If you suspect that this occurs, please read the Swedish Whistleblower Act, Chapter 1, Section 2 and the scope of the Whistleblower Directive in Article 2 and Annex Part 1 for applicable laws (or the equivalent legal space in the country you are reporting from).

2.3 Exceptions to the application

In Sweden, the Whistleblower Act does not apply to the reporting of information containing information classified under the Security Protection Act (2018:585), or information relating to national security. See Chapter 1, Section 3 of the Swedish Whistleblower Act.

3. How do I report?

If you see a need to report a misconduct, you should first contact your immediate manager, the business area manager or the company's HR function. We encourage everyone to be open about their identity. At the same time, we want to ensure that those who wish to report anonymously can do so. Therefore, we have a web-based whistleblowing service that enables anonymous reporting, see next section.

3.1 Written reporting

In case of a written report, we use our group-wide whistleblowing service VISSLAN. This service is always available through https://kamic-amplex-mindelon.visslan-report.se/. On the website, select "File New Report" and then describe the suspected misconduct by answering a number of questions

and using free text. Please describe what happened in as much detail as possible, as this will enable us to take appropriate action quickly. It is also possible to attach additional information and evidence in the form of written documents, images and audio files.

3.1.1 Sensitive personal data

Do not include sensitive data of persons mentioned in your report unless it is absolutely necessary to describe your case. Sensitive personal data are data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, a person's sex life or sexual orientation, genetic data and biometric data that can be used to uniquely identify a person.

3.1.2 Anonymity

You can remain anonymous throughout the reporting process without prejudice to your legal protection, but you also have the possibility to disclose your identity under strict confidentiality. Anonymity may in some cases hamper our ability to follow up on the case and take action, in which case we may later ask you to disclose your identity, also under strict confidentiality. However, we will always respect your wish to remain anonymous in the whistleblowing process.

3.1.3 Follow-up and logging in

After submitting your report, you will receive a sixteen-digit code, which you will need in the future to log in to VISSLAN from https://kamic-amplex-mindelon.visslan-report.se/. It is important that you save the code, otherwise you will not be able to access the case again. However, should you lose the code, you can create a new report referring to the previous, original report.

Within seven days, you will receive confirmation that a case handler has received your report. Case handlers are the independent and autonomous persons who receive cases through the online whistleblowing service, whose contact details can be found under the heading "6.1 Contact details for case handlers". From then on, you and the case handler can communicate through the tool's inbuilt anonymous chat function. Within three months, you will receive feedback on any actions taken or planned as a result of the report.

It is important that you log in regularly with your 16-digit code to answer any follow-up questions the case handler may have. In some cases, the case cannot be taken further without answers to such follow-up questions from you as the reporting person.

3.2 Oral reporting

It is also possible to submit an oral report via the whistleblowing service VISSLAN by uploading an audio file as an attachment when creating a case. To upload your file, select "Yes" to the evidence question. In the audio file, you describe the same facts and details as you would in a written report.

In addition, a physical meeting with the case handler can be requested via VISSLAN. This is most easily done by either requesting it in an existing case, or by filing a new report.

3.3 External reporting

We encourage you to always first whistleblow a misconduct internally, via our group-wide whistleblowing service, but should you for any reason consider it inappropriate, it is possible to initiate an external report. We then refer you to contact the competent national authority or, where

applicable, the competent EU institution, body or agency. Contact details to Swedish authorities are available via the following link: External reporting channels for whistleblowing.

4. What are my rights?

4.1 Right to confidentiality

You can remain anonymous throughout the reporting process, but if you choose to disclose your identity during the handling of the case, we will ensure that it is treated confidentially, and that no unauthorised person has access to information about who you are. We will not disclose your identity without your consent unless required by law.

4.2 Protection against retaliation

In the case of whistleblowing, there is statutory protection against negative consequences for the informant in the form of a prohibition of retaliation. However, this protection requires that the reporting person has reasonable grounds to believe that reporting the information is necessary to reveal a misconduct. The protection against retaliation also applies in relevant cases to persons in the workplace who assist the reporting person with information, as well as to colleagues and any relatives in the workplace.

This means that retaliation or the threat of retaliation because of whistleblowing is strictly prohibited. Examples of retaliation include dismissal, change of duties, reassignment, reduction in salary, imposed disciplinary measures or any other form of negative treatment related to the reporting of misconduct.

However, the protection against retaliation does not apply in cases where obtaining or disseminating the reported information is an illegal act in itself.

4.3 Publication of information

The protection against retaliation also applies to the publication of information. This assumes that you have first reported internally within the company or externally to a public authority, and that no appropriate action has been taken within 3 months (in some justified cases 6 months). The protection also applies when you disclose information without first reporting internally, or externally to a public authority, if you have reasonable grounds to believe that there is a clear danger to the public if the information is not disclosed, for example in an emergency situation where life and health are at risk, or where there is a risk that evidence may be concealed or destroyed.

4.4 Right to review documentation during meetings with case handlers

In the event that you have requested a meeting with the case handler(s) in a whistleblowing case, the case handler(s) will, with your consent, ensure that an accurate documentation of the meeting is kept in a durable and accessible form, either by recording the conversation or through written minutes or meeting notes.

We recommend that this documentation is saved and managed in the whistleblowing tool VISSLAN by the whistleblower creating a case where the information is securely collected and where the dialogue on the case can continue.

5. GDPR and handling of personal data

We comply with current legislation regarding the processing of personal data ("GDPR") and do our utmost to ensure the confidentiality in whistleblowing cases. Personal data not relevant to the case will therefore be deleted and the case will only be kept for as long as necessary. Our principle is not to keep information about a case for more than two years after its closure. For more information on our handling of personal data, please refer to our data protection policy available on the groups' websites https://amplexab.se, https://kamicgroup.com and https://www.mindelon.com.

6. Contact details

If you have questions about how we handle whistleblowing cases, you are always welcome to contact our case handlers.

6.1 Contact details for case handlers

Amplex, KAMIC Group and Mindelon's joint whistleblowing team consists of Jessika Axäll and Håkan Lundgren, with contact details as below.

Jessika Axäll
Head of Human Resources Amplex, KAMIC Group and Mindelon
jessika.axall@kamicgroup.com
+46 (0)8 759 35 51

Håkan Lundgren
Head of Corporate Development & Communications, Amplex, KAMIC Group and Mindelon
hakan.lundgren@kamicgroup.com
+46 (0)8 759 35 79

For cases received through the whistleblowing service VISSLAN and concerning our **Swedish companies**, we have an external recipient function through the **law firm Lindahl**. Lindahl receives whistleblowing cases, communicates with the whistleblower, makes an initial assessment of the case and then hands over the case, with a recommendation for further handling, to our internal whistleblower team as described above.

Contact details for the external recipient function at Lindahl Law Firm:

Mikael Mellberg
Lawyer/Partner
mikael.mellberg@lindahl.se
+46 (0)723 881 021

Ellinor Söderberg
Associate
ellinor.soderberg@lindahl.se
+46 (0)768 543 224

If necessary, additional individuals may be temporarily included in the whistleblowing team during the investigation of a case, to enable us to take appropriate action. These temporary resources assume the same responsibilities and confidentiality as the regular case handlers. However, a case will never be investigated by anyone who may have been involved in or directly affected by the potential misconduct.

6.2 Contact details for The Whistle Compliance Solutions AB
For technical questions about the whistleblowing tool VISSLAN, please contact The Whistle Compliance Solutions AB who developed VISSLAN. Contact details as below.

clientsupport@visslan.com
Customer service: +46 (0)10 750 08 10
Direct number (Daniel Vaknine, CEO): +46 (0)735 401 019

Visit Visslan's website for more information about VISSLAN.

7. Definitions

External reporting: Oral or written provision of information on misconduct to the competent authority(ies).

Feedback: Provision to reporting persons ("whistleblowers") of information on the actions planned or taken as follow-up and on the grounds for such follow-up.

Follow-up: Any action taken by the recipient of a report to assess the veracity of the allegations made in the report and, where appropriate, to address the reported breach, including through measures such as internal investigations, inquiries, prosecution, recovery measures and closure of the procedure.

GDPR: The General Data Protection Regulation (EU 2016/679), which is a European regulation governing the processing of personal data and the free flow of such data within the European Union.

Internal reporting: Oral or written provision of information on misconduct within a private sector organisation.

Misconduct: Acts and omissions that pose or have posed a serious threat or negative consequences to life, safety, health or the environment, or to public and private property and the economy.

Publication or **disclosure**: Making information available to the public.

Reporting: Oral or written submission of information on misconduct.

Reporting person: A natural person who reports or discloses information on misconduct acquired in the course of his/her work-related activities.

Retaliation: Any direct or indirect act or omission occurring in a work-related context and prompted by internal or external reporting or disclosure, which causes or is likely to cause unjustified harm to the reporting person.

VISSLAN: The Whistle Compliance Solutions AB's whistleblowing tool VISSLAN, which enables online reporting of misconduct.

Whistleblower Act: Swedish Act (2021:890) on the protection of persons reporting irregularities.

Whistleblower Directive: Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law.

This Whistleblowing Policy has been adopted by the Boards of Directors of Amplex, KAMIC Group and Mindelon. Changes to the policy may be decided by the Boards and/or Group Management. The policy is updated in October 2023.