

Whistleblowing policy

Preamble

Carat NV, having its registered office at Ambachtenstraat, 7, 2260 Westerlo, registered in the Crossroads Bank for Enterprises under number 0445.993.726, hereinafter referred to as “*the Company*” intends to conduct its businesses with integrity and ethics and therefore to provide with the possibility of reporting, under the terms and conditions described below, any breach of the legal and regulatory provisions referred to in article 1 of this Whistleblowing policy (hereinafter referred to as “*the Policy*”) when such breach is identified within the Company.

To this end, the Company provides a reporting channel KOKI Group is aware of its social responsibility in all its activities and bases this on generally valid, ethical values and principles. Sustainable management is also an essential part of the corporate culture. KOKI Group lives these principles and verifies compliance with them.

The reporting channel is governed by:

- the “*Rules of procedure for the whistleblowing procedure at Metabowerke GmbH*” (hereinafter referred to as “*the Rules of procedure*”), which will be updated from time to time, available on the following link:
https://www.metabo.com/t3/fileadmin/metabo/com_en/030_company/Rules_of_Procedure.pdf
- the page <https://www.carat-tools.com/be-nl> and <https://www.carat-tools.com/be-fr> explaining the available reporting channel through which reports can be submitted.
- the page <https://koki-group-eu.integrityline.app/> through which an online report can be made.
- any other Policy/Rules regarding Whistleblowing, which will be made available.

Insofar as this Policy applies to the Company, this Policy prevails over the rules set out in the Rules of procedure.

The purpose of this Policy is to encourage all staff members and anyone with a contractual relationship with the Company to disclose, under the terms and conditions described in this Policy, any reprehensible, illegal, unethical or fraudulent act involving the Company’s activities, without any fear of retaliation. In this Policy, the Company describes the procedure it recommends following in case of suspected breach and specifies the protection granted to whistleblowers.

In this framework, the Company is committed to comply with Directive 2019/1937 of 23 October 2019 on the protection of persons who report breaches under Union law, the Belgian law transposing it (hereinafter referred to as “*the Belgian Whistleblowers Act*”¹), and:

- to enable the confidential reporting, anonymously or otherwise, of any information relating to a potential or actual reprehensible act;
- to provide a high level of effective protection for the person making the report;
- to determine the procedure to be followed by the reporting person (“hereinafter referred to as “*the whistleblower*”);
- to take follow-up measures against inappropriate behaviour taking place within the Company.

¹ Law of 28 November 2022 on the protection of persons who report breaches of Union or national law within a legal entity in the private sector.

This Policy is available on the Company's website <https://www.carat-tools.com/be-nl> and <https://www.carat-tools.com/be-fr>.

Article 1. Material scope – which breaches can be reported?

1.1.

The reporting channel allow to signal suspected breaches in the following areas determined by the Belgian Whistleblowers Act:

- Public procurement
- Financial services, products and markets and prevention of money laundering and terrorist financing
- Product safety and compliance
- Transport safety
- Environmental protection
- Radiation protection and nuclear safety
- Food and feed safety, animal health and welfare
- Public health
- Consumer protection
- Protection of privacy and personal data, and the security of networks and information systems
- Fight against tax evasion
- Fight against social fraud

In addition, breaches affecting the financial interests of the Union can be reported, as well as breaches relating to the European internal market, including breaches of Union Competition and State aid rules.

A breach is defined as an act or omission that is unlawful or defeat the object or the purpose of the rules in the areas mentioned above. This includes any breach of the relevant legal or regulatory provisions or of the provisions adopted in application of the aforementioned provisions.

1.2.

In addition, and in view of the Company's and KOKI Group's commitment to conducting its business with integrity and ethics, and to being informed of any breaches perpetrated within it, the Company includes the following additional areas within the scope of this Policy:

- Violations of laws and regulatory requirements
- Violations of policies and guidelines
- Violations of its Codes of Conduct
- Indications of corruption and bribery
- Occupational health and safety violations
- Indications of bullying, discrimination and harassment
- Notes in connection with accounting and bookkeeping
- Violations of competition and antitrust law
- Violations of human rights
- Violation of international trade controls
- Conflict of interest
- Miscellaneous

The reporting channel are not available for general complaints, customer complaints or warranty inquiries.

Article 2. Personal scope – who can report breaches?

The reporting channel aim to handle reports from the following persons (*“the whistleblowers”*) who acquired information on breaches in a work-related context:

- persons having the status of employees;
- persons having self-employed status;
- shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members, as well as volunteers and paid or unpaid trainees;
- any persons working under the supervision and direction of contractors, subcontractors and suppliers;
- persons where they report information on breaches acquired in a work-based relationship which has since ended;
- 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;
- any person in possession of information obtained outside a professional context concerning breaches committed within the Company with regard to financial services, products and markets.

Article 3. The report

Any person referred to in article 2 may report, via the reporting channel referred to below, information, including reasonable suspicions, about actual or potential breaches or risks related thereto, which occurred or are very likely to occur or attempts to conceal such breaches.

Breaches means acts or omissions that are unlawful and relate to the areas mentioned under article 1 or defeat the object or the purpose of the rules foreseen in the areas mentioned under article 1.

Article 4. Reporting channel

Any person referred to in article 2 who has knowledge of or reasonable grounds to suspect a breach within the Company in the areas referred to in article 1 is invited to report it directly via the reporting channel.

4.1. Internal reporting channel

4.1.1. Available internal reporting channel

The following channel is available to whistleblowers for reports:

Online	Koki-group-eu.integrityline.app/
--------	---

If the whistleblower wishes to make a report anonymously², this is possible via the online reporting system³. Even anonymous communication with the whistleblower is possible via this online reporting

² We however encourage the whistleblower to provide his name in the report.

³ How is the anonymity of the whistleblower protected?

When submitting a report or question via the Integrity Line, the whistleblower remains anonymous unless he decides to disclose his identity. Provided the whistleblower does not enter any data himself that would allow conclusions to be drawn about his identity, the system protects his anonymity with a certified technical solution.

His report is kept anonymous by encryption and other security solutions. In addition, the system does not store IP addresses and computer IDs and does not use cookies. However, if a report is created from a computer in the company network, there is a risk that the websites visited will be saved in the browser or company history. To eliminate this risk, the whistleblower can create the report from a computer that

system. The Company therefore recommends that whistleblowers using the online reporting system to log in regularly and to check their own case for new messages.

Reports via the online reporting system are free of charge.

If a report relates to a specific company of the KOKI Group the whistleblower can select this company in the online reporting system and thus enable the report to be processed by this company.

The channel is designed, established and operated in a secure manner that ensures that the confidentiality of the identity of the whistleblower and any third party mentioned in the report is protected and prevents access thereto by non-authorised staff members. The channel ensures the protection of the privacy and personal data of the whistleblower and of any third party mentioned in the report at all times.

4.1.2. Processing of reports

A. Notification

The whistleblower needs to go to the start page and click on the "Make a report" button.

On the next page, the whistleblower formulates his report in his own words and answers questions about the case he has observed (select an answer or enter his own text). He can also attach a file to support his report or record a sound clip. The whistleblower needs to remember that files can contain information about the author (metadata).

The whistleblower can submit a report using his name or anonymously. Then the whistleblower must set up his own secure mailbox⁴ (see "Secure Inbox"). This mailbox will help him receive feedback and answer any questions we may have.

The whistleblower will then be asked to answer a security question to prove that he is not a "robot".

B. Content of the report

Reports should contain the following information:

- What is your suspicion (Description of the incident – what happened when and where and is the incident still ongoing, etc.)?
- In which company did the incident occur?
- Where did the incident occur (country, city, event, etc.)?
- Is the whistleblower an employee of the company concerned, supplier, customer, etc.?
- What is the name of the affected department?
- Who is involved in the incident (potential suspicious person)?

is not part of the company network. If the whistleblower uploads documents, he should also be aware that the files may contain metadata that could reveal the identity of the report creator. Therefore, he should ensure that all metadata is removed from the files before uploading them.

⁴ Via the secure mailbox, the Company provides the whistleblower with a technical space that is only accessible to the whistleblower and the Company. The Company can contact the whistleblower via the secure mailbox. This is important because questions often arise in the course of processing which the Company can only clarify with whistleblower's help and which can be decisive for the further procedure. When the whistleblower creates a secure mailbox, the whistleblower will be assigned a Case ID and will need to choose a password. The whistleblower must use this Case ID and password to access the mailbox and to check whether he has received any questions. Via the secure mailbox, the Company will give you feedback on what happens with the report.

If the whistleblower wishes, all communication with the Company will remain anonymous.

- Did anyone observe the incident (witnesses)?
- Is there any evidence to prove the incident (e.g. documents etc.)?

C. What happens after the report?

▪ Recipient of the report

All reports are sent via the online reporting channel secure servers to the Chief Compliance Officer of Metabowerke GmbH and his representatives and/or, if available, to a locally / regionally responsible Compliance Officer and his representatives: Please note that the Company has its own local designated person who receives reports concerning the Company and will deal with these reports. They act independently, confidentially and without conflict of interests or instructions.

If the Chief Compliance Officer of Metabowerke GmbH, his representatives, and the locally / regionally responsible Compliance Officer and his representatives or other employees have a conflict of interest or if the violation was committed by one of these persons themselves, this person will be immediately excluded from the investigation.

▪ Confirmation of receipt

The whistleblower receives a confirmation of receipt of the report within 7 days from the day the report is received if he has provided with his contact details or has set up a communication option.

▪ Follow-up of the report

- Checking the report

A follow-up will be done by the recipient of the report.

'Follow-up' means any action taken by the recipient of the report to assess the accuracy (/admissibility) of the allegations made in the report (i.e. whether an incoming report falls under the abovementioned scope of application, if this is not the case, the whistleblower receives corresponding feedback) and, where relevant, to address the breach reported, including through actions such as:

- an (internal) investigation;
- prosecution;
- an action for recovery of funds;
- or the closure of the procedure (if by assessing the accuracy (/admissibility) of the report, the recipient of the report reaches the conclusion that the incident may not be reported via the whistleblower system).

- Clarification of the facts

The recipient of the report maintains contact with the whistleblower for the purpose of providing feedback and requesting further information where necessary for instance if the facts need to be clarified (in which case the recipient of the report will contact the whistleblower via the Integrity Line or via other communication channels, if made available by the whistleblower).

It may be necessary to involve other specialist departments, such as Human Resources, Data Protection, Purchasing, etc., or external service providers.

If necessary, law enforcement authorities are involved, which may be the case in particular if there is a legal obligation to do so or if further clarification of the facts is no longer possible through internal measures but appears necessary.

In the event of concrete suspicious activity reports, specialists can be called in and an investigation initiated.

- **Investigation**

If the report is confirmed, the report will be promptly and thoroughly investigated in accordance with this Policy. All investigations will be conducted thoroughly, taking into account the principles of confidentiality, data protection, impartiality and equity to all concerned.

- **Measures**

Appropriate measures will be examined and, if necessary, taken and followed up.

This may involve sanctions against employees, such as a warning, reprimand or dismissal, whereby the nature and severity of the breach and culpability will of course be given due consideration.

If necessary, criminal charges will be filed. It may also be necessary to assert claims for damages.

Remedial measures are intended to prevent or stop the breach, or at least minimise it if it is not possible to prevent or stop it.

Furthermore, it is examined whether preventive measures can be taken or expanded and implemented if necessary.

D. Feedback

At the latest 3 months from the acknowledgement of receipt or, if no acknowledgment was sent to the whistleblower, three months from the expiry of the seven-day period after the report was made, the whistleblower will receive a feedback on the measures planned or already taken and the grounds for the choice of that follow-up, if he has provided with his contact details or has set up another means of communication. Confidential information can be communicated in order to guarantee a feedback.

E. Conclusion of the procedure - storage

At the end of the procedure, the results and measures taken are documented and stored in an access-protected manner. The statutory deletion and retention obligations are observed.

4.2. External reporting channels

Alternatively to the internal reporting channel, the whistleblower may report the suspected breach via external reporting channels, such as those made available by the Belgian competent authorities⁵, after

⁵ French

1° le Service public fédéral Economie, PME, Classes Moyennes et Energie ;

2° le Service public fédéral Finances ;

3° le Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement ;

4° le Service public fédéral Mobilité et Transports ;

5° le Service public fédéral Emploi, Travail et Concertation sociale ;

having first reported through the internal reporting channel, or by directly reporting through external reporting channels.

These authorities are designated to receive external reports, give feedback to the reporting person, and to carry out the duties provided for in the Belgian Whistleblowers Act, in particular as regards follow-up.

The Federal Ombudsmen are responsible for coordinating reports done via external channel. In short, they will also be responsible for receiving external reports, checking that they are admissible and

6° *le Service public de programmation Intégration Sociale, Lutte contre la Pauvreté, Economie Sociale et Politique des Grandes Villes ;*

7° *l'Agence fédérale de Contrôle nucléaire ;*

8° *l'Agence fédérale des médicaments et des produits de santé ;*

9° *l'Agence fédérale pour la sécurité de la chaîne alimentaire ;*

10° *l'Autorité belge de la Concurrence ;*

11° *l'Autorité de protection des données ;*

12° *l'Autorité des services et marchés financiers ;*

13° *la Banque nationale de Belgique ;*

14° *le Collège de supervision des réviseurs d'entreprises ;*

15° *les autorités visées à l'article 85 de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces ;*

16° *le Comité national de sécurité pour la fourniture et la distribution d'eau potable ;*

17° *l'Institut belge des services postaux et des télécommunications ;*

18° *l'Institut National d'Assurance Maladie-Invalidité ;*

19° *l'Institut National d'Assurances Sociales pour Travailleurs Indépendants ;*

20° *l'Office National de l'Emploi ;*

21° *l'Office National de Sécurité Sociale ;*

22° *le Service d'Information et de Recherche Sociale ;*

23° *le Service autonome de Coordination Anti-Fraude (CAF) ;*

24° *le Contrôle de la Navigation.*

Dutch

1° *de Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie;*

2° *de Federale Overheidsdienst Financiën;*

3° *de Federale Overheidsdienst Volksgezondheid, Veiligheid van de voedselketen en Leefmilieu;*

4° *de Federale Overheidsdienst Mobiliteit en Vervoer;*

5° *de Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg;*

6° *de Programmatie Overheidsdienst Maatschappelijke Integratie, Armoedebestrijding, Sociale Economie en Grootstedenbeleid*

7° *het Federaal Agentschap voor Nucleaire Controle;*

8° *het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten;*

9° *het Federaal Agentschap voor de veiligheid van de voedselketen;*

10° *de Belgische Mededingingsautoriteit;*

11° *de Gegevensbeschermingsautoriteit;*

12° *de Autoriteit voor Financiële diensten en Markten;*

13° *de Nationale Bank van België;*

14° *het College van toezicht op de bedrijfsrevisoren;*

15° *de autoriteiten gemeld in artikel 85 van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;*

16° *het Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater;*

17° *het Belgisch Instituut voor postdiensten en telecommunicatie;*

18° *het Rijksinstituut voor ziekte- en invaliditeitsverzekering;*

19° *het Rijksinstituut voor de Sociale Verzekeringen der Zelfstandigen;*

20° *de Rijksdienst voor Arbeidsvoorziening;*

21° *de Rijksdienst voor Sociale Zekerheid;*

22° *de Sociale Inlichtingen en Opsporingsdienst;*

23° *de Autonome dienst Coördinatie Anti-Fraude (CAF);*

24° *de Scheepvaartcontrole.*

transmitting them to the competent authority for investigation, which will depend on the matter of the report.

If an authority which has received a report does not have the competence to address the breach reported, this authority transmits it to the Federal Ombudsmen who transmits the report to the competent authority, within a reasonable time, in a secure manner.

If no authority considers itself competent to receive a report, the Federal Ombudsmen act as the competent authority to receive external reports.

The contact details of the Federal Ombudsman are as follows:

Address: Rue de Louvain, 48, box 6 1000 Brussels
Online complaint: <https://www.mediateurfederal.be> / <https://www.federaalombudsman.be>
E-mail: contact@mediateurfederal.be / contact@federaalombudsman.be
Phone: 0800 99 961 or +32 2 289 27 27 from abroad
Fax number: +32 2 289 27 28

We recommend prioritising the internal reporting channel where possible. In case of an external report, the protection measures against retaliation are only guaranteed if the conditions specified in article 5.2.3 are met.

Article 5. Protection for whistleblowers

5.1. Confidentiality

The identity of the whistleblower is treated under strict confidentiality throughout the procedure and will not be disclosed to anyone beyond (1) the persons competent to receive the report and ensure its follow-up, and beyond (2), unless a legal exception will apply, the person concerned by the report within a reasonable timeframe, due to Data Protection requirements, not exceeding one month from the report unless there is a legal obligation to disclose⁶ or the whistleblower provides consent to disclose.

This shall also apply to any other information from which the identity of the whistleblower may be directly or indirectly deduced.

All internal and external parties involved in the investigation and follow-up are bound by an obligation of confidentiality.

5.2. Protection against retaliation

5.2.1. Protected persons

Any person referred to in article 2 cannot be subject to retaliation, including threats of retaliation and attempts of retaliation, because of the facts reported. The protection against retaliation shall also apply to the following persons if they had reasonable grounds to believe that the whistleblower fell within the scope of the Belgian Whistleblowers law:

⁶ The identity of the whistleblower may be disclosed where this is a necessary and proportionate obligation imposed a special law in the context of investigations by national authorities or judicial proceedings, including with a view to safeguarding the rights of defence of the person concerned (i.e. "a natural or legal person who is referred to in the report or public disclosure as a person to whom the breach is attributed or with whom that person is associated"). In this case, the whistleblower shall be informed before its identity is disclosed, unless such information would jeopardise the related investigations or judicial proceedings.

- facilitators;
- third persons who are connected with the whistleblower and who could suffer retaliation in a work-related context, such as colleagues or relatives of the whistleblower; and
- legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context.

Retaliation is defined as any direct or indirect act or omission prompted by an internal or external report or a public disclosure, which causes or may cause an unjustified prejudice to reporting person.

5.2.2. Retaliation measures

Unless duly justified, the following can constitute retaliation measures:

- Employment measures, e.g. suspension, lay-off, dismissal, salary reduction, refusal to grant a promotion, change of roles, disciplinary sanctions or measures, reprimand or other penalty including a financial penalty, demotion, withholding of promotion, low or negative performance review or employment reference;
- Decisions having negative consequences on work conditions, e.g. transfer of duties, change of location of place of work, reduction in wages, suspension of training, change in working hours, leave refusal;
- Certain behaviours, e.g. coercion, intimidation, harassment, ostracism, discrimination, disadvantageous or unfair treatment;
- Failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
- Failure to renew, or early termination of, a temporary employment contract;
- Harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- Blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- Early termination or cancelation of a contract for delivery of services or products;
- Exclusion or suspension of a member or its appointed delegate;
- Cancellation of a licence or permit;
- Psychiatric or medical referrals.

5.2.3. Conditions of the protection – what if the content of the report subsequently turns out to be false?

Protection against retaliation is guaranteed provided the following conditions are satisfied:

- The whistleblower acted in good faith at the time the report was submitted, i.e. he had reasonable grounds to believe that the information reported on the breach were true and that the breach fell under the scope of this Policy.
- The whistleblower must have reported according to the present Policy and the Belgian Whistleblowers Act.

The first criterion is assessed in relation to a person in a similar situation with comparable knowledge. It is important that the whistleblower believes or assumes at the time of reporting that the content is true and that he does not submit this report with abusive intent. The whistleblower is not expected to look for evidence or clarify the incident himself. It may therefore be that the investigation later reveals that no offense has been committed. In this case, the whistleblower shall not lose the benefit of protection solely on the grounds that the report made in good faith has proved to be inaccurate or unfounded.

In case of abusive, opportunistic reporting or in bad faith or in case of reporting made with the sole aim of harming the Company or third parties, the whistleblower may incur disciplinary sanctions (including sanctions provided by the Work rules), legal actions or criminal sanctions⁷.

It is forbidden to impede a report. Any person who impedes a whistleblower to submit a report also incurs disciplinary sanctions (including sanctions provided by the Work rules), legal actions or criminal sanctions⁸.

Article 6. Data protection

Personal data communicated through the whistleblowing procedure are processed by **Carat NV**, having its registered office at Ambachtenstraat, 7, 2260 Westerlo, registered in the Crossroads Bank for Enterprises under number 0445.993.726.

The Company collects and processes such personal data in compliance with the legislation on the protection of whistleblowers, including the Belgian Whistleblowers Act, and the legislation on data protection, including Regulation 2016/679 (the “GDPR”).

This data processing is carried out in the framework of compliance with a legal obligation and/or the legitimate interest of the Company, insofar as the internal reporting channel exceeds the legal objectives, in particular the detection of crimes and the guarantee of the Company safety and ethical conduct.

The relevant data protection information can be found on the online reporting system:

<https://koki-group-eu.integrityline.app/app-page;appPageName=Privacy%20policy?lang=en>
<https://koki-group-eu.integrityline.app/app-page;appPageName=Privacy%20policy?lang=nl>

Further data protection information is available on the following website:

<https://www.carat-tools.com/be-nl/content/privacy>
<https://www.carat-tools.com/be-fr/content/privacy>

Article 7. Entry into force

This Policy comes into force on 16/12/2025 for an indefinite period of time.

The Company reserves the right to amend this Policy at any time, including, but not limited to, in the event of changes in relevant legislation and/or operational requirements.

⁷ Where it can be shown that someone knowingly reported or publicly disclosed wrong information, criminal penalties can be incurred under articles 443-450 of the Belgian criminal code, and civil damages can be claimed (cf. art 33, § 3 of the Belgian Whistleblowers Act).

⁸ Impeding someone to file a Report or taking retaliation measures are punished by prison sentences between 6 months and 3 years and/or a fine between 600 and 6000 Euro. The penalty can be pronounced against the Company and/or members of its staff (cf. art 33, § 2 of the Belgian Whistleblowers law).