Whistleblowing Policy

1 Purpose

Vanbreda Risk & Benefits - including its affiliated companies as listed in the Appendix - (hereinafter referred to as “the Company”) is committed to acting with integrity and ethics in its operations and is therefore committed to ensuring that its employees have the opportunity, in accordance with the terms and conditions set forth below, to report in the most serene and confidential manner possible any identified or suspected breaches in the Company of the legal and regulatory standards referred to in Section 2.2 of this policy.

The company’s own employees are often the first to have knowledge of threats or breaches occurring within a company. However, they might be stopped from expressing their concerns or suspicions for fear of reactions or reprisals.

However, this potential fear could ultimately result in the Company being kept in the dark about possible breaches and being unable to take the necessary steps to address them. Consequently, this could undermine the interests of the Company, which pursues high standards of good governance and business ethics.

The purpose of this policy is to prevent this situation by strongly encouraging all employees or former employees and other persons who have a contractual relationship with the Company to report any breach or illegal, unethical or fraudulent activity related to the Company’s business without fear of penalties or other actions.

This policy is adopted in accordance with the Act of November 28, 2022 on the protection of persons who report breaches of national or Union law within legal entities in the private sector, transposing the European Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019 on the protection of persons who report breaches of Union law, hereinafter referred to as “the Act”.

The purpose of this policy is to:

- enable the confidential, anonymous or otherwise, reporting of information about possible or actual breaches;
- offer protection to persons reporting a breach or assisting the reporting person;
- establish the procedure to be followed for this purpose by the person reporting a breach.

This policy is available on the Company’s website and on the intranet, and may be amended from time to time.

Naturally this policy in no way precludes direct dialogue and communication of information outside the reporting procedure. The Company wishes to emphasise that employees with concerns or suspicions may contact their line managers, the Human Resources department, the confidential counsellors or the Compliance department at any time.

2 Scope

2.1 Who is covered by this policy?

This policy applies to the following individuals:

- employees
- persons working on a self-employed basis
- temporary employees such as service providers or agency staff
- volunteers and interns (paid or unpaid);
- shareholders and members of the Company's administrative, management or supervisory body (including non-executive members);
- any person who works or has worked under the supervision and direction of contractors, subcontractors and/or suppliers of the Company;
- anyone who has information about breaches in the Company in the area of financial services, products and markets, even outside a work-related context.

This policy also applies to reporting persons whose working relationship has ended or is yet to begin if they obtained information about breaches during or after the termination of the working relationship or during the recruitment process or other pre-contractual negotiations.

2.2 Which breaches can be reported?

Only breaches can be reported that relate to any of the following areas as defined in the Act:

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

In addition, breaches can be reported that may affect the financial interests of the European Union as well as breaches relating to the European internal market including Union rules on competition and state aid.

Breach means an act or omission that is unlawful or defeats the purpose or application of the rules in the above areas. It means any breach of the relevant legal or regulatory provisions or the provisions adopted in pursuance of the aforementioned provisions.

3 Reporting

3.1 Purpose of the reporting

Any breach relating to the areas referred to in Section 2.2 as well as any information about such breaches, including any reasonable suspicion of actual or potential breaches that have occurred or are very likely to occur within the Company, and attempts to conceal such breaches within the Company, may be reported in writing or orally through any one of the channels referred to in Section 4.

3.2 Conditions for reporting and protection of reporting persons

The report must be made in good faith and must not be based on mere hearsay or gossip, nor may the report be made with the purpose of harming the Company.

The reporting person must have reasonable grounds to believe that the information on breaches reported was true at the time of reporting.

If the report contains false, unsubstantiated or opportunistic allegations, or is made for the sole purpose of harming or injuring others, the Company may take appropriate disciplinary and/or legal action against the reporting person, including the imposition of penalties in accordance with the Company's rules.

4 Reporting channels

Any person covered by this policy who has information about actual or suspected breaches referred to in Section 2.2 is encouraged to report this to the Company as soon as possible in good faith and in accordance with the principles set forth in Section 3.2.

4.1 Internal reporting channels

4.1.1 Who may use the internal reporting channels?

All employees or other persons covered by this policy may use the internal reporting channels provided by the Company.

4.1.2 Which channels are available?

1-
Breaches may be reported by means of the reporting tool made available for this purpose which can be accessed:

- by a link on the intranet;
- by an Internet link on Vanbreda's website.

Reporting should preferably be done in Dutch, French or English. Any report made in another language will have to be translated first as it may affect the accuracy of the report content.

These reporting channels are accessible at all times, 24/7.

The reporting tool can be used to request a face-to-face meeting or telephone conversation with the whistleblowing officer as noted below in Section **4.1.4** of this policy.

Each of the above channels is operated in a confidential and secure manner to ensure the confidentiality of the identity of the reporting person and any third parties named in the report. Access to the channels is strictly limited to employees who have access to them on the basis of their responsibilities and/or authority.

4.1.3 Reporting procedure

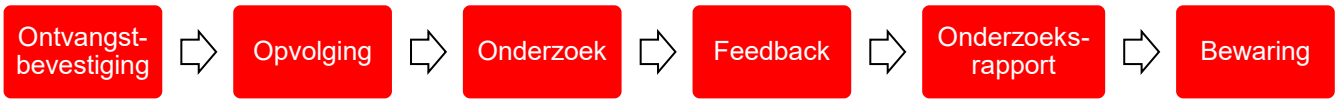
A report shall include a brief description of reasonable suspicions concerning an actual or potential breach of any of the domains listed in Section 2.2 that has occurred or is very likely to occur as well as any attempts to conceal or disguise such breaches.

The report can be made anonymously or otherwise at the reporting person's discretion by indicating this in the reporting tool.

The report must be sufficiently detailed and documented and must include the following information (where the relevant information is known):

- a detailed description of the events and how they came to the attention of the reporting person;
- the date and place of the event;
- the names and positions of the persons concerned, or information that allows their identification;
- the names of other persons, if any, who can corroborate the facts reported;
- when making a report, the name of the reporting person (this information is not requested if an anonymous report can be made); and
- any other information or elements that may help the investigating team to verify the facts.

4.1.4 What happens after reporting?



1-Acknowledgement of receipt
The reporting person will receive an acknowledgement of receipt within 7 days of reporting. A case number is also provided for the purpose of following up on the report.

2-Follow-up
Follow-up means any action taken by the recipient of a report to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, including through actions as an internal enquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure.

The whistleblowing officer follows up on reports, maintains communication with the reporting person and, where necessary, asks for further information from and provides feedback to the reporting person, and receives any new reports.

3-Investigation
The whistleblowing officer may decide whether or not to investigate a report after consulting with the management within the organisation.

The report will be investigated promptly and carefully in accordance with this policy. All investigations will be conducted thoroughly in accordance with the principles of confidentiality, impartiality and fairness towards all persons concerned. The whistleblowing officer will, if necessary, set up an investigating team. The investigating team is given authority in accordance with the existing policies within the Company.

Persons involved in the breaches or potential breaches reported by the reporting person are excluded from the investigating team, nor are they allowed to participate in the assessment of the report or the determination of the actions to be taken regarding the report.

Conflicts of interest are reported to the board of directors if the management/executive board is targeted in the report. The general meeting of the Company is notified if the board of directors appears to be involved.

4-Feedback
The whistleblowing officer will give the reporting person appropriate feedback within a reasonable timeframe, not exceeding three months from the acknowledgement of receipt of the report. This feedback contains information for the reporting person about the actions envisaged and/or taken and the grounds for these actions. The whistleblowing officer informs the reporting person through the chosen internal reporting channel.

5-Investigation report
Upon completion of the investigation, the investigating team prepares a summary report, describing the investigative measures carried out. A drafted, non-confidential and anonymised version of this summary report may be shared, on a need-to-know basis only, outside the investigating team with the local or executive management in order to reach a final decision.

A member of the investigative team prepares a final report describing the facts and the final decision:

i. If the (potential) breach is proven, relevant actions will be identified with a view to counteracting the (potential) breach and protecting the Company; or
ii. If the investigation shows that there is insufficient or no evidence of a (potential) breach, no further action will be taken.

The reporting person is informed of the closure of the report and the decision made through the chosen internal reporting channel.

4.1.5 **Whistleblowing officer**

The following person is designated as the Company's whistleblowing officer: General Manager Audit.

The whistleblowing officer carries out his/her duties independently and without conflict of interest. He/she is bound by a duty of confidentiality.

4.1.6 **Record keeping of the reports**

The Company keeps a record of all reports received, in accordance with the confidentiality measures set forth in Section 5.1 of this policy.

These reports and the related information will be retained for as long as the contractual relationship between the reporting person and the Company lasts.

Where a recorded telephone line or another recorded voice messaging system is used for reporting, subject to the consent of the reporting person, the Company will document the oral reporting in one of the following ways:

- by making a recording of the conversation in a durable and retrievable form; or
- through a complete and accurate transcript of the conversation prepared by the whistleblowing officer. The reporting person will be given the opportunity to check, rectify and agree the transcript of the call by signing it.

Where an unrecorded telephone line or another unrecorded voice messaging system is used for reporting, the Company will document the oral reporting in the form of accurate minutes of the conversation written by the staff member responsible for handling the report. The reporting person will be given the opportunity to check, rectify and agree the minutes of the conversation by signing them.

If a face-to-face meeting takes place with the whistleblowing officer, complete and accurate records of the meeting will be kept in a durable and retrievable form, subject to the reporting person's consent. The Company has the right to document the meeting in one of the following ways:

- by making a recording of the conversation in a durable and retrievable form;
- through accurate minutes of the meeting. The reporting person will be given the opportunity to check, rectify and agree the minutes of the conversation by signing them.

4.2 External reporting channels

1-
Reporting persons may use an external reporting channel after reporting through the internal channels or directly through the external reporting channels if they deem it more appropriate.

2-
The Federal Coordinator is charged by Belgian law with coordinating reports filed through external channels.

He/she is responsible for receiving external reports, checking their admissibility and forwarding them to the competent authority for investigation, which will be different depending on the subject of the report.

This authority could be, for example, the FPS Policy & Support (in the area of public procurement), the Financial Services and Markets Authority (FSMA), the National Bank of Belgium (NBB) or the Supervisory Board of Auditors (in the area of financial services, products and markets), the FPS Economy (in the area of consumer protection), the Data Protection Authority (in the area of privacy and personal data protection), etc.

In exceptional cases, the Federal Coordinator may also conduct the detailed investigation.

The Federal Coordinator's contact details are:

Address: Leuvenseweg 48 box 6, 1000 Brussels
Online complaint: https://www.federaalombudsman.be/nl/klachten/dien-een-klacht-in
Email: contact@federaalombudsman.be
Phone: 0800 99 961

5 Protection measures

The Company is committed to making every effort to provide appropriate and effective protection to the persons covered by this policy to the extent that the reporting complies with the terms of the Act, in particular by taking the following measures:

5.1 Assurance of confidentiality

The Company guarantees to take the necessary steps to ensure that employees and other persons concerned by this policy can file a report with the Company in full confidence.

The Company undertakes to put in place the necessary measures to ensure that the identity of the reporting person is not disclosed to anyone beyond the authorised staff members competent to receive or follow up on reports, without the free and explicit consent of that person.

This also applies to any other information from which the identity of the reporting person may be directly or indirectly deduced.

Notwithstanding the previous paragraph, the identity of the reporting person may be disclosed where this is necessary and proportionate under special legislation in the context of investigations by national authorities or judicial proceedings, in particular with a view to safeguarding the rights of defence of the person concerned.

In the latter case, the reporting person will be informed before his or her identity is disclosed, unless such information would jeopardise the related investigations or judicial proceedings. This is the case,

for example, when the reporting person represents an important witness in court or in cases of unjustified or wrongful reporting to protect the rights of defence of the person concerned.

5.2 Protection against retaliation

Any form of retaliation against the persons referred to in Section 2.1 who enjoy protection under this policy, including threats of retaliation and attempts of retaliation, is prohibited, in particular in the form of:

- suspension, lay-off, dismissal or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties, change of location of place of work, reduction in wages, change in working hours;
- suspension or withholding of training;
- negative performance assessment or employment reference;
- imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;
- coercion, intimidation, harassment or 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 reporting person will not, in the future, find employment in the sector or industry;
- early termination or cancellation of a contract for goods or services;
- cancellation of a licence or permit;
- psychiatric or medical referrals.

6 Processing of personal data

For the purposes of the internal reporting procedure, the Company is considered the data controller for the processing of personal data.

Any processing of personal data pursuant to this policy will be carried out in accordance with the applicable personal data protection laws, including the European General Data Protection Regulation (GDPR).

The following personal data may be processed in the context of a report: name, position, date of employment, contact information and email address of the reporting person and of persons involved in the breach, any identified or identifiable information provided by the reporting person and collected in the context of the internal investigation. This processing of data is done in the context of complying with a legal obligation and/or the legitimate interest of the Company, to the extent that the internal reporting channel exceeds legal objectives, in particular the detection of breaches, ensuring the security and ethical conduct of the Company.

Personal data which are manifestly not relevant for the handling of a report will not be collected or, if accidentally collected, will be deleted without undue delay. Relevant data will be kept until the breach

reported is expired, unless legal obligations require a longer period (as in the case of professional liability).

The identity of the reporting person can only be disclosed with the consent of the reporting person. Other information also remains strictly confidential and can only be shared on a strict need-to-know basis.

Personal data will not be transferred to recipients located in countries outside the European Economic Area (EEA) whose laws do not provide the same level of data protection.

All persons whose personal data are processed in the context of breach reports have the right to access and copy, right to rectification, right to data erasure, right to object and right to lodge a complaint with the supervisory authority in accordance with applicable law. However, these rights may be limited by the rights and freedoms of others, in particular the reporting person's right to confidentiality and the Company's right to proper follow-up on the report.

For more information on the processing of personal data, please refer to the Privacy Notices for employees, job applicants, independent service providers and agency workers, and the Privacy Policy available on the Company's intranet.

7 Modifications

The Company reserves the right to modify this policy at any time, including but not limited to changes in relevant legislation and/or operational needs.

Vanbreda Risk & Benefits, including affiliated companies, comprises the following companies:

Vanbreda Risk & Benefits NV
Plantin en Moretuslei 297, 2140 Antwerp
Company number 0404.055.676

Vanbreda Accounting Services BV
Justus Lipsiusstraat 46c, 3000 Leuven
Company number 0561.946.932

Vanbreda Agencies NV
Plantin en Moretuslei 309, 2140 Antwerp
Company number 0772.859.673

Vanbreda Ausloos NV
Justus Lipsiusstraat 46c, 3000 Leuven
Company number 0474.182.421

Vanbreda Cornelis NV
Hundelgemsesteenweg 306, 9820 Merelbeke
Company number 0425.054.196

Vanbreda Credinco NV
Plantin en Moretuslei 297, 2140 Antwerp
Company number 0462.175.702

Vanbreda Dekerf NV
Statiestraat 84, 1740 Ternat
Company number 0451.680.203

Vanbreda Geerts NV
Looyweg 1, 2310 Rijkevorsel
Company number 0466.513.679

Vanbreda Huysmans NV
Veemarkt 1, 2800 Mechelen
Company number 0478.505.552

Vanbreda Mediùs NV
Plantin en Moretuslei 297, 2140 Antwerp
Company number 0406.096.042

Vanbreda Simplex NV
Plantin en Moretuslei 297, 2140 Antwerpen,
Company number 0473.851.334

Vanbreda Soenen Missinne NV
Gasthuisstraat 81, 8970 Poperinge
Company number 0405.513.151

Justitia NV
Plantin en Moretuslei 301, 2140 Antwerp
Company number 0404.479.211

Pensiontheker Benefit Outsourcing / Partner in Benefits
Gravendreef 11/6, 9120 Beveren
Company number 0674.961.068