



GREENYARD

WHISTLEBLOWING POLICY

Copyright © 2022 Greenyard unpublished material. All rights reserved. This policy contains proprietary and confidential information belonging to Greenyard. Reproduction, disclosure, or use of any portion of this policy without express written authorisation from Greenyard is strictly prohibited. This restriction applies to the information on every page of the policy. Contents may be disclosed only to authorised Greenyard employees for the purpose of performing their responsibilities. Printed or other physical representations of this document are classified as “for reference only.”

TABLE OF CONTENT

1 OBJECTIVE	4
2 WHAT IS WHISTLEBLOWING?	4
3 WHAT MISCONDUCT TO REPORT?	4
3.1 Misconduct	4
3.2 Reporting in good faith	5
4 WHEN AND HOW TO REPORT?	5
4.1 Reporting channels	5
4.2 What information to be included in a whistleblowing report.....	6
5 WHAT MEASURES ARE IN PLACE TO PROTECT THE WHISTLEBLOWER?	7
5.1 Confidentiality of the Whistleblower’s identity	7
5.2 Anonymity.....	7
5.3 No retaliation.....	8
6 WHAT IS THE INTERNAL FOLLOW-UP PROCESS?	8
6.1 Acknowledgement of receipt	8
6.2 Investigation	8
6.3 Feedback.....	10
6.4 Report.....	10
6.5 Decision	10
6.6 Record keeping	10
7 WHISTLEBLOWING DATA PROTECTION NOTICE	11
7.1 In general	11
7.2 What types of personal data do we process?	11
7.3 Why do we process your personal data?	11
7.4 With whom do we share your personal data?	12
7.5 How long do we keep your personal data?	13
7.6 What do we do to keep your personal data safe?	13
7.7 What are your rights?	13
7.8 Questions or complaints?	13
SCHEDULE 1 – EXAMPLES OF CONDUCTS TO BE REPORTED	14

1 OBJECTIVE

Greenyard is committed to the highest standards of business ethics and legal compliance.

It is therefore of great importance to Greenyard to have relevant procedures in place to enable the reporting of any concern about actual or suspected misconduct within Greenyard's operations in a responsible and effective manner, whilst remaining protected from retaliation.

This Policy is in line with the section "Reporting of Breaches" of Greenyard's Code of Conduct.

This Policy addresses the following questions:

- What is whistleblowing?
- What Misconduct to report?
- When and how to report?
- What measures are in place to protect the Whistleblower?
- What is the internal follow-up process?
- How are personal data being processed?

2 WHAT IS WHISTLEBLOWING?

Whistleblowing means the confidential or anonymous reporting by Greenyard employees or external parties (e.g. customers, suppliers, etc.) of illegal, dishonest or wrongful conduct within Greenyard's operations, while being protected from retaliation.

The person reporting the Misconduct is the "**Whistleblower**".

3 WHAT MISCONDUCT TO REPORT?

3.1 Misconduct

A Whistleblower may report illegal, dishonest or wrongful conduct such as (but not limited to)

- (i) a crime or misdemeanour,
- (ii) an infringement of governing laws, regulations and/or international treaties,
- (iii) an infringement of Greenyard's contractual commitments,
- (iv) an infringement of Greenyard's Code of Conduct and/or other policies and procedures,
- (v) any other type of unethical or dishonest behaviour (the "**Misconduct**").

Schedule 1 provides some examples of Misconduct.

A report under the Whistleblowing Policy must be made in the general interest of the Greenyard group. Personal grievances and complaints on unacceptable behaviour at work or excessive workload are not excluded from being reported under the Whistleblowing Policy. However, given the personal nature of such a report the internal follow-up process may deviate from the current Policy. The Confidant will nevertheless hear the complaint and will provide information about the applicable local policies and the channels available through which such complaints can be addressed.

3.2 Reporting in good faith

When submitting a report, a Whistleblower must always act in good faith and the report must be based on reasonable grounds. When the reporting contains false, unfounded or opportunistic allegations, or is made for the sole purpose of defaming or causing damage to others, Greenyard may take appropriate disciplinary and/or legal measures against the Whistleblower.

A Whistleblower is not responsible for investigating the Misconduct or for determining corrective measures. This task is assigned to qualified case handlers performing the relevant internal functions (see Section 6).

4 WHEN AND HOW TO REPORT?

If you discover, become aware of, or have reasonable grounds to suspect (potential) Misconduct taking place within Greenyard's operations, you are encouraged to immediately notify Greenyard of the incident concerned.

Before reporting under this Policy, you are invited to first consider using normal reporting channels (i.e. your direct line manager or supervisor, your General Manager or Managing Director or your local HR manager). If for any reason, you feel uncomfortable or reluctant reporting through the normal reporting channels, Greenyard's internal whistleblower tool provides you with an alternative channel through which you can report the Misconduct confidentially or anonymously.

4.1 Reporting channels

4.1.1 Internal whistleblowing channels

Within Greenyard an internal online whistleblower tool ("**Whistleblower Tool**") is available through which a Whistleblower can report Misconduct to corporate office ("Group Reporting Channel") or to the local organisation ("Local Reporting Channel")¹ or both channels simultaneously ("Local/Group Reporting Channel").

When submitting the report, the Whistleblower must choose whether the Misconduct should be investigated locally and/or by corporate office. The Whistleblower Tool provides the option to submit the report to

- the Local Confidant within the local organisation (see Schedule 2 for the list of Local Confidants);
- Corporate Legal & Compliance; or

¹ The Local Reporting Channel is generally available in local organisations within the Greenyard group that employ more than 49 workers. In the absence of a Local Confidant, a report can only be submitted through the Group Reporting Channel.

- both the Local Confidant and Corporate Legal & Compliance.

Reporting via the online tool can be done in writing or orally. A Whistleblower may also use the Whistleblower Tool to request a meeting for making an oral report with its Local Confidant or with Corporate Legal & Compliance.

4.1.2 External reporting channels (European Union)

It is strongly recommended to first consider reporting Misconduct through the normal reporting channels or via the Whistleblower Tool within Greenyard (see Section 4.1.1). Internal reporting remains the most efficient route to allow Greenyard to thoroughly investigate the matter and adopt appropriate measures addressing the Misconduct.

Within the European Union, a Whistleblower has the option to report Misconduct falling within the scope of Directive (EU) 2019/1937 to a local competent authority who is responsible for receiving and investigating whistleblowing reports (external reporting). The list of local competent authorities and references to the procedures and safeguard measures for reporting externally is attached in Schedule 3.

4.2 What information to be included in a whistleblowing report

A report must be sufficiently detailed and documented, and should include the following details (when the relevant information is known):

- a detailed description of the events and how it came to the Whistleblower's attention;
- the date and place of the event;
- the names and job positions of the persons involved, or information that enables their identification;
- the names of other persons, if any, who can attest to the reported facts;
- when submitting a report, the Whistleblower's name (such information will not be requested when an anonymous report is made); and
- any other information or element that could help the investigating team to verify the facts.

A Whistleblower is strongly invited to submit a report and to include their name. This facilitates the internal investigation as well as putting in place the requisite measures for the Whistleblower's protection (see Section 5).

5 WHAT MEASURES ARE IN PLACE TO PROTECT THE WHISTLEBLOWER?

Greenyard wants to create a safe environment where a Whistleblower feels comfortable reporting any Misconduct within the organisation. To that end the following protective measures were put in place:

- the confidential treatment of the identity of the Whistleblower;
- the possibility for the Whistleblower to remain anonymous when submitting a report;
- the prohibition of any form of retaliation against the Whistleblower and related parties.

5.1 Confidentiality of the Whistleblower's identity

The Whistleblower's identity will be treated as strictly confidential. The following measures have been adopted in order to ensure such strict confidential treatment:

- Reports are managed by case handlers and files are kept within the dedicated Whistleblower Tool, which is only accessible to authorized individuals of the investigation team;
- All internal and external parties involved in the investigation and in follow-up actions are subject to strict confidentiality obligations. Unauthorised disclosure of information relating to the investigations, the report or the identity of a Whistleblower will not be tolerated and will result in disciplinary action. Depending on the circumstances, such conduct may also give rise to other actions, including civil or criminal lawsuits.

The Whistleblower's identity will **not** be disclosed, except

- (i) when the Whistleblower explicitly consents to the disclosure; or
- (ii) disclosure is required by law. Depending on the type of reported Misconduct, it may be legally required to involve the public authorities to initiate an official investigation. In such cases, Greenyard may be required to report the name of the Whistleblower to the public authorities, while preserving the Whistleblower's strict confidentiality at all times. Greenyard will inform the Whistleblower when its identity has been reported, except where such disclosure would jeopardize the investigations or judicial proceedings.

5.2 Anonymity

A Whistleblower has the option to remain anonymous when submitting a report and during the subsequent investigations. In such case, the Whistleblower Tool guarantees that the identity of the Whistleblower remains protected and cannot be uncovered by anyone involved in the investigation.

Greenyard has put in place the following measures to guarantee the Whistleblower's anonymity:

- the Whistleblower will at no time be requested to reveal their identity;

- the Whistleblower Tool guarantees that the identity of the Whistleblower is protected and that there is no means whatsoever to find out about their identity;
- the Whistleblower can throughout the follow-up process refuse to answer questions which they feel could identify themselves.

Greenyard will undertake all reasonable efforts to investigate an anonymous report, but notes that in some cases there are limitations of what can be achieved when the Whistleblower chooses to remain anonymous.

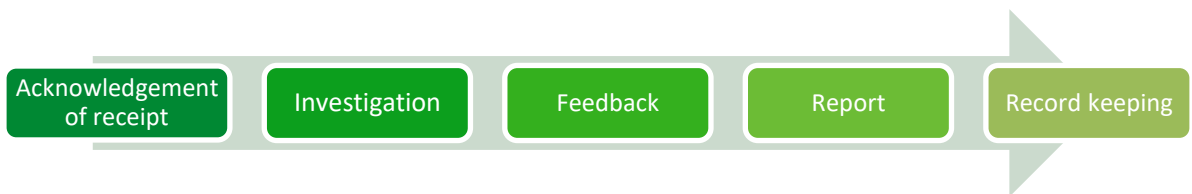
5.3 No retaliation

Any type of retaliation, threat, penalty or discrimination against the Whistleblower, third persons connected with the Whistleblower (e.g. colleagues or relatives) or anyone having assisted the Whistleblower to submit a report or having participated in the investigation will not be tolerated. Greenyard will take appropriate action against anyone who retaliates or threatens to retaliate.

In case a Whistleblower, third persons connected with the Whistleblower or anyone who assisted the Whistleblower is worried they may face retaliation or feels they already have been retaliated against, they should immediately escalate their concerns to Corporate Legal & Compliance (see Schedule 4 for the contact details).

Corporate Legal & Compliance will investigate the matter in all neutrality and make sure the appropriate actions are taken to prevent or remedy the retaliatory actions.

6 WHAT IS THE INTERNAL FOLLOW-UP PROCESS?



6.1 Acknowledgement of receipt

Within seven days of receipt of the report, a case handler will send an acknowledgement of receipt to the Whistleblower via the Whistleblower Tool.

6.2 Investigation

The report will be promptly and diligently investigated in accordance with this Policy. All investigations will be undertaken thoroughly and in observance of the principles of confidentiality, impartiality and fairness towards all individuals involved. The case handler may get in contact with the Whistleblower to obtain more information and/or evidence about the Misconduct. Where needed for conducting a thorough and confidential investigation, external parties (eg. external counsel, investigative firms, accounting firms, etc.) may be involved.

The case handler and team responsible for the investigation depends on whether the Whistleblower submitted the report to the Local Confidant, Corporate Legal & Compliance or both.

6.2.1 Local Confidant

When the report was submitted to the Local Confidant, the investigation is undertaken at local level. Representatives of local HR² may be involved on a strict need-to-know basis. Together they form the local investigation team.

Where the Misconduct reveals a more structural problem or involves multiple group companies, the Local Confidant may seek the assistance of Corporate Legal & Compliance and Internal Audit or Corporate HR, subject to the confidential treatment of the identity of the Whistleblower. The identity of the Whistleblower can only be revealed to Corporate Legal & Compliance, Internal Audit or Corporate HR with the explicit written consent of the Whistleblower.

6.2.2 Corporate Legal & Compliance

When the report was submitted to Corporate Legal & Compliance, the investigation is undertaken at corporate level. Corporate Legal & Compliance takes the lead on the investigation and may involve Internal Audit and Corporate HR on a strict need-to-know basis. Together they form the corporate investigation team. Local HR will only be involved in the investigation, subject to the confidential treatment of the identity of the Whistleblower. The identity of the Whistleblower will only be revealed to local HR with the explicit written consent of the Whistleblower.

6.2.3 Local Confidant and Corporate Legal & Compliance

When the report was submitted to both the Local Confidant and Corporate Legal & Compliance, the Local Confidant and Corporate Legal & Compliance must consult each other and decide who should take the lead on the investigation taking into account the type of Misconduct and the individuals involved.

Local HR, Internal Audit or Corporate HR may get involved in the investigation on a strict need-to-know basis.

6.2.4 Conflicts of interest

Individual(s) involved in the Misconduct reported by the Whistleblower will be excluded from the investigation team, and will also not be allowed to participate in the consideration of the report or the determination of what action, if any, needs to be taken regarding the report.

If such involvement excludes the majority of the investigation team from participating in the process, the task to consider the report and determine appropriate action will be assigned by

² Local HR refers to the local HR function or in the absence of a local HR function, to local management with HR responsibilities.

the Chairman of the Audit Committee of Greenyard NV to an investigating officer who is not subject to such conflicts of interest.

6.3 Feedback

Not later than three months after the acknowledgement of receipt, the Whistleblower will receive feedback through the Whistleblower Tool about the (ongoing or concluded) investigation of his report.

6.4 Report

Upon conclusion of the investigation, the investigation team will prepare a summary report describing the investigative measures that were carried out. A redacted non-confidential and anonymized version of this summary report may be shared outside the investigation team (see above Point 6.2) with local, division or executive management, on a need-to-know basis only, in order to come to a final decision.

6.5 Decision

The investigation team together with local, division or executive management (as appropriate) will make a final decision as to whether the Misconduct is proven and will define the relevant actions needed to terminate the Misconduct and to protect the company.

A member of the investigation team will draft a final report with a description of the facts and the final decision taken:

- i. In the event the Misconduct is proven, relevant actions will be defined with a view to terminate the Misconduct and to protect the company; or
- ii. In the event the investigations conclude that there is insufficient or no evidence for the Misconduct, no further action will be taken.

The Whistleblower is informed through the Whistleblower Tool about the conclusion of the report and the decision taken.

6.6 Record keeping

Records of the reports submitted by the Whistleblower will be kept in the Whistleblower Tool ensuring strict confidential treatment of the report.

When a report is submitted orally through the online form, the case handler will prepare a transcript of the recording to facilitate the handling of the report. When a report is submitted orally during a meeting at the request of the Whistleblower, the case handler will prepare minutes of the meeting. In the case of oral reporting, the Whistleblower will receive the opportunity to check and rectify the transcript or minutes of the meeting and upon agreement will be requested to sign them.

Any record will be kept no longer than what is necessary and proportionate and will be deleted 2 years after the investigation has been closed.

The investigation must be considered closed (i) when it was decided not to take any further action, or (ii) when all action items defined in the final decision were implemented or completed. In the event the report results in legal actions or proceedings, the investigation must be considered closed upon expiry of all time limits for legal remedies or upon exhaustion of those remedies.

7 WHISTLEBLOWING DATA PROTECTION NOTICE

This Policy, in particular this section, is intended to inform you and to comply with our legal obligations in respect of data protection and whistleblowing. If you are a Whistleblower, a person reported or another third party mentioned, we process personal data about you. This section about data protection explains how your personal data will be processed for the purposes of this Policy.

7.1 In general

Your personal data is processed by us (Greenyard NV, Strijbroek 10, 2860 Sint-Katelijne-Waver) as data controller or by any another entity belonging to the Greenyard group, when necessary to process your report. For the provision of the internal reporting channel (Whistleblower Tool), we use a service provider who is considered to be the data processor and recipient of your personal data.

You may contact us with respect to questions relating to the processing of your personal data via e-mail at dataprivacy@greenyard.group.

7.2 What types of personal data do we process?

When you are either the Whistleblower, the person reported or another third party mentioned, we process the information reported to us. This could include your name, title, relation to us, information about misconduct, criminal offences, or suspicion thereof, and information about sanctions. Also, the reported information may include other special categories of personal data such as information on race and ethnic origin, information on political beliefs, information on religious or philosophical beliefs, information on trade union affiliation, health information and information on sexual relations or sexual orientation. Where the Whistleblower has chosen to submit the report anonymously, the report contains no information that we can link to the Whistleblower.

7.3 Why do we process your personal data?

We will only process the above-mentioned types of personal data, to the extent such personal data is provided to us. In addition, we will process is to handle, investigate and follow-up on the report, including the investigation of allegations mentioned in the report. The processing of your personal data for these purposes are based on our legitimate interest in creating a safe and pleasant working environment and to keep our business operations safe and secure. Please note that if the report concerns breaches of EU law, it is our legal obligation to process the above-mentioned personal data. Also, if the report concerns breaches of specific labour

laws designed to ensure well-being at work, we may be legally obliged to process such personal data.

If the report mentions special categories of personal data, we rely, depending on the content of the report, on the necessity of processing these data based on an overriding public interest, the vital interests of the data subject if he or she is physically or legally incapable of giving consent, or on the necessity of processing these data for occupational health purposes.

In addition to these purposes, we can also process your personal data for the following purposes:

Purposes	Legal basis
To comply with legal obligations or to comply with any reasonable request from competent law enforcement agents or representatives, judicial authorities, governmental agencies or bodies, including competent data protection authorities.	To comply with a legal obligation.
To transfer your personal data to the police or judicial authorities as evidence if there are justified suspicions of an unlawful act or crime committed by you.	To comply with a legal obligation.
To establish or exercise legal claims or organise our defence.	Our legitimate interest to defend ourselves in the context of legal proceedings.

7.4 With whom do we share your personal data?

In principle we will not share your personal data with anyone but trusted case handlers working for us, as well as our supplier of the internal reporting channel (Whistleblower Tool). Anyone who has access to your personal data will always be bound by strict legal or contractual obligations to keep your personal data safe and confidential. This means that only the following recipients will receive your personal data:

- you;
- trusted case handler(s);
- governmental or judicial authorities insofar we are required to send them your personal data (e.g. tax authority, police or law enforcement);
- supplier of the internal reporting channel.

The supplier of the internal reporting channel transfers your personal data outside the European Economic Area (the European Economic Area consists of the EU, Liechtenstein, Norway and Iceland), but we will take adequate safeguards to protect your personal data when transferred.

7.5 How long do we keep your personal data?

Your personal data will only be processed as long as necessary to achieve the purposes described above. In any event, we will delete personal data relating to a report or investigation in accordance with section 6.6 of this Policy, unless we are required to retain it for a longer period in connection with legal proceedings.

7.6 What do we do to keep your personal data safe?

The security and confidentiality of your personal data we process is very important to us. Hence, we have taken steps to ensure that all personal data processed are kept safe. These steps include processing only the personal data required for achieving the purposes we have communicated to you. We have also taken technical and organisational measures to secure the internal reporting channel (Whistleblower Tool).

7.7 What are your rights?

You have the right to be provided with information about your personal data, which is processed by us and, if certain legal requirements are satisfied, rights to rectification, erasure, and restricted processing, as well as the right to object to data processing. If you would like to exercise your rights, please contact us at the e-mail address mentioned below.

7.8 Questions or complaints?

If you have a question or complaint regarding how we process your personal data, please feel free to contact us by e-mail at dataprivacy@greenyard.group. You also have the right to file a complaint with the competent data protection authority.

SCHEDULE 1 – EXAMPLES OF CONDUCTS TO BE REPORTED

This list mentions examples of illegal, dishonest or wrong conducts that can be reported. This list is not exhaustive.

Matter	Example of Misconduct
Product and food safety, product integrity	<ul style="list-style-type: none"> • You are forced by your manager to release products exceeding food safety norms, such as certain microbiological norms, without formal approval from the Quality department; • You know that a product labelled “Organic” and claiming ingredients from German origin are actually not organic and are not from German origin. After having first thought that it is a mistake, you reported it to your manager, who justified the false labelling with economic reasons;
Transport safety	<ul style="list-style-type: none"> • You notice that some of Greenyard’s truck drivers do not respect the mandatory restrictions regarding driving times;
Public health and environment	<ul style="list-style-type: none"> • You notice that the fertilizer used by one of our suppliers is forbidden since it pollutes the soil – the persons in charge at Greenyard are aware of this but ignore it;
Data protection and security of network system	<ul style="list-style-type: none"> • You notice that one of your colleagues, having access to the personal data of employees of Greenyard, sells it to a third company for commercial purposes;
Competition and anti-trust	<ul style="list-style-type: none"> • You attend a meeting between Greenyard and two of its main competitors – The purpose of the meeting is to agree on fixed prices for some products – this is illegal as this agreement is a cartel, strictly forbidden by competition law;
All forms of financial malpractices or impropriety such as fraud, corruption, bribery and theft	<ul style="list-style-type: none"> • You are requested by your superior to pay invoices but you know the amount is highly superior to the amount of the delivered goods – you are not convinced by the explanations given by your superior when you confronted him/her;
Discrimination and harassment	<ul style="list-style-type: none"> • A colleague told you being the victim of a group of other colleagues, who are constantly making fun of him and his work – your colleague is in great distress; • One of your co-workers continuously makes sexist remarks to a colleague

Prevention of money laundering, terrorist financing	<ul style="list-style-type: none"> You notice that funds coming from a company we have no active business with, are transiting via Greenyard to be redistributed to a subsidiary of this company;
Insider trading	<ul style="list-style-type: none"> You hear one of your “insider” colleagues telling by phone to someone he/she knows that the financial results of Greenyard are not good and that he would better sell his shares now;
Corporate or tax arrangements, accounting, auditing matters	<ul style="list-style-type: none"> You notice that, via its foreign subsidiaries, Greenyard is committing systematic tax avoidance;
Social media	<ul style="list-style-type: none"> You see on LinkedIn that a group of your colleagues is disclosing a lot of details about a project you know is confidential – you shared your concern with your colleagues but they refuse to remove the post, arguing that it is good for their CV;
Public procurement - bribery	<ul style="list-style-type: none"> You are requested by your superior to send to a public officer a very expensive watch with a short note stating that “Greenyard hopes to have the pleasure to collaborate” with the public officer in a near future.
<p>More broadly, the following types of behaviour can also be reported:</p> <ul style="list-style-type: none"> Failure to comply with legal obligations, statutes, and regulatory directives; Any form of criminal activity; Improper conduct or unethical behaviour that undermines universal and core ethical values such as integrity, respect, honesty, accountability and fairness; Non-disclosure of conflicting interests; Attempt to conceal any illegal, dishonest or wrongful conduct 	