Roveg Fruit BV

Data Protection Information Policy

1.0 Purpose

Accompanied by the whistleblowing channel, a data protection information policy has to be created for the proper use and protection of personal data received via the whistleblowing channel of Roveg Fruit BV established by the Whistleblowing Policy.

2.0 Scope

Since the whistleblowing channel is open for anyone working within the organisation, the scope of the information of data protection also covers anyone that makes a report through the channel. Therefore, it applies to employees, suppliers, third parties or retailers, or if you are involved in any way with any part of our operations.

3.0 Policy statement

The whistleblowing system provides a channel through which we can securely and confidentially receive and process information regarding any alleged or suspected misconduct or wrongdoing. These also include any violation to our Code of Conduct, Ethics Business Policy, Supplier Code of Conduct or any other internal policy. Any report regarding violations to law or regulations that applies to us because the nature of our business is also covered.

Any personal data submitted with a report made through the whistleblowing channel will be processed in accordance with the requirements of the European General Data Protection Regulation (GDPR) and Dutch Whistleblower Protection Law.

Personal Data is processed based on Roveg's legitimate interest on identifying and preventing misconduct, wrongdoings or violations, particularly breaches of applicable laws or our own ethical standards. Additionally, the implementation of the whistleblowing system aligns with the Dutch Whistleblower Protection Law as it provides a safe and confidential framework where the confidentiality of reports is a mandate, there is a proper safeguarding of personal data, and it aligns with GDPR's requirements on processing, security and data subjects' rights.

The processing of the whistleblower's personal data is based on their consent (Art. 6 (1) a GDPR). Consent is considered voluntary, as whistleblowers have the option to submit their report anonymously if they prefer. Consent can also be revoked. However, this is generally only possible within one month of submitting the report. In certain cases, we may be required under Art. 14 (3) a GDPR to inform the accused party within one month about the allegations and the ongoing investigation. In exceptional situations, the revocation period

may be shorter, such as when the nature of the report needs immediate involvement of authorities or courts, in which case the personal data will be stored with the respective authority's or court's case files. Revoking consent does not affect the lawfulness of any processing that occurred based on the consent before it was revoked.

3.1 Personal data process

The data that we process is only the data that the whistleblower has voluntarily provided throughout the whistleblowing channel when submitting a report. The personal data and information that can be processed, if provided, are:

- name;
- contact information;
- the fact that a report was made using the whistleblower channel;
- the fact that the whistleblower is an employee of Roveg Fruit BV, if applicable;
- names and other personal data of the people involved in the situation that were mentioned in the report, if applicable.

The responsible for data processing is:

Roveg Fruit BV
Nijverheidsweg 20
2742 RG Waddinxveen
The Netherlands
Email: whistleblowing@roveg.nl

After your report is send, the information will be received and reviewed only by authorized employees within Roveg's HR department who are obliged to work impartially and independently. Your report and any other information submitted will be treated confidentially. Due to the nature of the violation, the investigation can entail multiple actions depending on each case such as reviewing documents, conducting interviews, making an audit or such other. If there is a risk of human and/or environmental rights violation, further investigation and action will follow, which may include involving external authorities.

In every step of the investigation, your data will be stored encrypted and password-protected and will only be disclosed to the extent necessary to conduct a full and fair investigation or as required by applicable laws. In certain exceptional cases, we may be legally required under Art. 14 (3) a GDPR to inform the accused party of the allegations against them. However, this obligation only arises if disclosing the information will no longer negatively impact the investigation. Even in such situations, we will protect your identity as the whistleblower to the fullest extent allowed by law.

If false information is intentionally or negligently provided with the purpose of harming someone's reputation or a report was done in bad faith, we cannot guarantee confidentiality entirely.

3.2 Data storage

We will retain your personal data for as long as it is necessary for the investigation and final evaluation of the reported concern, as well as for any legitimate reasons to keep it (e.g., for potential legal proceedings), or if required by applicable laws. Once these purposes are fulfilled, the data will be deleted in accordance with legal regulations. Additionally, if your report is found to be unfounded, your personal data will be deleted immediately.

3.3 Rights under data protection law

As a whistleblower, your personal data and the people involved in your report have various data subject rights, according to the European data protection law. You can stand a claim on this regard by contacting the responsible for data processing in this matter. The rights that are applicable are:

- Right of access (Art. 15 GDPR)
- Right of rectification (Art. 16 GDPR)
- Right to erasure (Art. 17 GDPR)
- Right to restrict processing (Art. 18 GDPR)
- Right to complain to a data protection authority
- Right to object (Art. 21 GDPR)

If you decide to make an objection, we will immediately assess to what extent the storing of the data is still necessary. Data that is no longer necessary will be immediately deleted.

4.0 Roles, responsibilities and delegations

ROLE	RESPONSIBILTY
ICT	Manages the proper functioning of the whistleblowing channel and system
HR	Engagement with employees/workers, executing policy, progress on targets and KPIs
Sustainability team	Engagement with employees/workers, yearly review and update of policy, quality control of progress on targets and KPIs

5.0 Document Control

5.1 Key Information

Title	Data Protection Information Policy
Document number	Provided by relevant team

Purpose	A data protection information policy has to be created for the proper use and protection of personal data received via the whistleblowing channel of Roveg Fruit BV established by the Whistleblowing Policy.
Audience (Select)	Internal & Public
Category (Select)	G- Governance
UN Sustainable Development Goals (SDGs)	This document aligns with Sustainable Development Goal/s: SDG 8: Decent Work and Economic Growth & SDG 16: Peace, Justice, and Strong Institutions.
Approval date	18 October 2024
Effective date	18 October 2024
Review date	Yearly – revision to be performed alongside the update of KPIs associated to this policy
Policy advisor	Human Resources officer/manager, Sustainability officer
Approving authority	Kirsten Weijts (HR Manager), Henk Roodenburg (CEO)

5.2 Revision History

Version	Date	Summary of Changes	Initials	Changes Marked
1.0	October 11th 2024	First Version	V.G.	No

6.2.1 Version Numbering

The Version numbering system to be used within Roveg ESG is the system that is based on the use of version numbers with points to reflect major and minor changes to a document.
The version number of a document in a draft format will start at 0.1 reflecting its draft status and then progress through revision by incrementing the number to the right of the point. The version number will convert to 01.0 upon the document/record receiving all required approvals, and deemed ready for publishing.

For example a document with the version number 0.1 is in draft format. When the document has been approved and authorized ready for publishing the version number will start at 01.0, and the number will only be modified after the first minor amendment to become 01.1. Each major revision to the document will result in the number to the left of the point incrementing by one and the number to the right of the dot point will return to zero e.g. 02.0.

The benefit of version control number is at a glance the document will provide a great deal of information. If the version number of the document is 01.0 then you know that there have been no changes since the

document was authorised and published. A version number on a document of 03.5 would reflect that there had been two major changes and five minor revisions to the document since it was last reviewed. Therefore, indicating that the document has been kept current and reviewed on a regular basis. The version number should always be displayed clearly on the front cover of the document.

7.0 Related Policy Documents and Supporting Documents

Legislation	General Data Protection Regulation - GDPR https://gdpr-info.eu/ Dutch Whistleblower Protection Act | Wet bescherming klokkenluiders
Policy	Whistleblowing Policy - Roveg
Procedures	N/A
Local Protocol	N/A
Forms	Whistleblowing Policy - Roveg